MARC KRASNER

Sur la théorie de la ramification des idéaux de corps non-galoisiens de nombres algébriques

Thèses de l'entre-deux-guerres, 1938

<http://www.numdam.org/item?id=THESE_1938__202__1_0>

N° de la série : 1776

Série : A

N° d'ordre : 2642

THÈSES

PRÉSENTÉES A LA

FACULTÉ DES SCIENCES DE L'UNIVERSITÉ DE PARIS

POUR OBTENIR LE GRADE DE

DOCTEUR ÈS SCIENCES MATHÉMATIQUES

PAR

MARC KRASNER

LICENCIÉ ÈS SCIENCES

1ère THÈSE. — **Sur la théorie de la ramification des idéaux de corps non-galoisiens de nombres algébriques.**

2me THÈSE. — **Propositions données par la Faculté.**

Soutenues le février 1938 devant la Commission d'examen :

MM. MONTEL, Président,
GARNIER, VALIRON } Examinateurs.

FACULTÉ DES SCIENCES DE L'UNIVERSITÉ DE PARIS

MM.

Doyen honoraire . . M. MOLLIARD.

Doyen . . . . . C. MAURAIN, *Professeur*, Physique du Globe.

Professeurs honoraires . H. LEBESGUE. A. FERNBACH. Émile PICARD. GUILLET. PÉCHARD. Léon BRILLOUIN. FREUNDLER. AUGER. BLAISE. DANGEARD. LESPIEAU. MARCHIS. VESSIOT. PORTIER. MOLLIARD. LAPICQUE. G. BERTRAND. ABRAHAM. Ch. FABRY. Léon BERTRAND. WINTREBERT. DUBOSCQ. BOHN.

PROFESSEURS

M. CAULLERY . . .	T	Zoologie (Évolution des êtres organisés).
G. URBAIN.	T	Chimie générale.
Émile BOREL. . . .	T	Calcul des probabilités et Physique mathématique.
Jean PERRIN	T	Chimie physique.
E. CARTAN	T	Géométrie supérieure.
A. COTTON	T	Recherches physiques.
J. DRACH	T	Analyse supérieure et Algèbre supérieure.
Charles PÉREZ . . .	T	Zoologie.
E. RABAUD	T	Biologie expérimentale.
M. GUICHARD. . . .		Chimie minérale.
Paul MONTEL . . .	T	Théorie des fonctions et Théorie des transformations.
L. BLARINGHEM. . .	T	Botanique.
G. JULIA	T	Mécanique analytique et Mécanique céleste.
C. MAUGUIN	T	Minéralogie.
A. MICHEL-LÉVY . .	T	Pétrographie.
H. BÉNARD	T	Mécanique expérimentale des fluides.
A. DENJOY.	T	Application de l'analyse à la Géométrie.
L. LUTAUD	T	Géographie physique et géologie dynamique.
Eugène BLOCH . . .	T	Physique théorique et physique céleste.
G. BRUHAT.		Physique.
E. DARMOIS.		Enseignement de Physique.
A. DEBIERNE	T	Physique générale et Radioactivité.
A. DUFOUR	T	Physique (P. C. B.).
L. DUNOYER		Optique appliquée.
A. GUILLIERMOND .	T	Botanique.
M. JAVILLIER. . . .		Chimie biologique.
L. JOLEAUD.		Paléontologie.
ROBERT-LÉVY. . . .		Zoologie.
F. PICARD.		Zoologie (Évolution des êtres organisés).
Henri VILLAT. . . .	T	Mécanique des fluides et applications.
Ch. JACOB	T	Géologie.
P. PASCAL	T	Chimie minérale.
M. FRÉCHET	T	Calcul différentiel et Calcul intégral.
E. ESCLANGON. . . .	T	Astronomie.
Mme RAMART-LUCAS	T	Chimie organique.
H. BÉGHIN	T	Mécanique physique et expérimentale.
FOCH.		Mécanique expérimentale des fluides.
PAUTHENIER		Physique (P. C. B.).
DE BROGLIE.	T	Théories physiques.
CHRÉTIEN.		Optique appliquée.
P. JOB		Chimie générale.
LABROUSTE		Physique du Globe.
PRENANT		Zoologie.
VILLEY		Mécanique physique et expérimentale.
COMBES		Botanique (P. C. B.).
GARNIER.	T	Mathématiques générales.
PÉRÈS.		Mécanique des fluides.
HACKSPILL		Chimie (P. C. B.).
LAUGIER.		Physiologie générale.
TOUSSAINT.		Technique Aéronautique.
M. CURIE		Physique (P. C. B.).
G. RIBAUD.	T	Hautes températures.
CHAZY.	T	Mécanique rationnelle.
GAULT.		Chimie (P. C. B.).
CROZE.		Recherches. Physiques.
DUPONT.	T	Théories chimiques.
LANQUINE.		Géologie.
VALIRON.		Mathématiques générales.
BARRABÉ.		Géologie structurale et géologie appliquée.
MILLOT.		Zoologie (P. C. B.).
F. PERRIN		Théories physiques.
VAVON.		Chimie organique.
G. DARMOIS.		Calcul des probabilités et Physique mathématique.
CHATTON	T	Biologie maritime.
AUBEL		Chimie biologique.
Jacques BOURCART. .		Géographie physique et Géologie dynamique.
Mme JOLIOT-CURIE. .		Physique générale et Radioactivité.
PLANTEFOL		Biologie végétale (P. C. B.).
CABANNES.		Enseignement de Physique.
GRASSÉ		Biologie animale (P. C. B.).
PRÉVOST.		Chimie (P. C. B.).

Secrétaire . . . . . A. PACAUD.

Secrétaire honoraire . . . . . D. TOMBECK

SUR LA THÉORIE

DE LA

RAMIFICATION DES IDÉAUX DE CORPS NON-GALOISIENS DE NOMBRES ALGÉBRIQUES

PAR

M. KRASNER

BRUXELLES

HAYEZ, IMPRIMEUR DE L'ACADÉMIE ROYALE DE BELGIQUE

112, rue de Louvain, 112

—

1937

Extrait des *Mémoires*
publiés par la Classe des Sciences, de l'Académie royale de Belgique.
Collection in-4°. Deuxième série, Tome XI, 1937

INTRODUCTION

Quand à la fin du siècle précédent on eut surmonté les dernières difficultés de la théorie générale des corps de nombres algébriques, en particulier la question de facteurs premiers du discriminant, on pouvait distinguer dans cette théorie deux parties, dont la liaison était des plus lâches :

1° Partie arithmétique, appelée encore « théorie d'idéaux », qui était basée sur les notions de la divisibilité et de l'idéal, dont les fondateurs ont été Kummer, Dedekind, Kronecker, Dirichlet;

2° Partie algébrique, dite encore « théorie de Galois », un peu plus ancienne que la précédente, basée sur les notions de l'isomorphisme et du groupe, dont les fondateurs ont été Lagrange et surtout Ev. Galois.

Ce fut M. D. Hilbert [1] [et dans les cas les plus simples, en même temps, Dedekind [2] et Frobenius [3]] qui, dans sa *Théorie de corps galoisiens*, étudia pour la première fois la liaison très profonde qui existe entre les propriétés arithmétiques d'idéaux premiers de ces corps et les propriétés de structure de leur groupe. Il attacha pour cela à chaque idéal premier d'un corps galoisien une suite caractéristique des sous-groupes du groupe de Galois de ce corps. On sait quels grands services a rendus la théorie de M. Hilbert dans l'étude des corps de nombres algébriques. Elle était

---

[1] *Gött. Nachr.*, 1894, pp. 224-236; *Jahresb. d. Deutsch.-Math. Ver.*, t. 4, 1894-1895, pp. 175-546.

[2] *Gött. Nachr.*, 1894, pp. 272-277.

[3] *Sitz.-ber. d. Akad. zu Berlin*, 1896, pp. 6, 13, 124, 129, 130.

devenue l'instrument indispensable et, très souvent, l'étoffe même de toutes les recherches postérieures, aussi bien de celles de la théorie générale de corps galoisiens de nombres algébriques, que de celles qui se rapportaient aux corps de nature particulière.

La théorie de M. Hilbert est très simple pour les idéaux non ramifiés des corps galoisiens. Par contre, elle se complique et devient très intéressante pour certains idéaux ramifiés. Elle leur fait correspondre une suite caractéristique d'entiers positifs, dits nombres de ramification. Les travaux qui ont suivi celui de M. Hilbert sont surtout consacrés à l'étude de cette suite; ce sont :

1° Les travaux de MM. Fueter (4), Speiser (5) et Ore (6), qui sont consacrés à l'étude de congruences, inégalités et égalités auxquelles satisfont les nombres de ramification, et de la liaison qui existe entre les valeurs de ces nombres et la structure des groupes caractéristiques d'un idéal. M. Ore étudie, de plus, dans ces travaux, la structure d'équations d'Eisenstein définissant un corps $\mathfrak{p}$-adique, et, en particulier, il étudie dans certains cas simples la forme qu'on peut donner à ces équations par une transformation de Tschirnhausen.

2° Travail de M. Herbrand (7), consacré à l'étude du rapport entre les groupes et les nombres caractéristiques d'un idéal premier d'un corps galoisien K et ceux de l'idéal premier correspondant d'un sous-corps galoisien $\overline{K}$ de K, ainsi qu'aux questions analogues pour les idéaux des corps composés.

3° Travail de M. Hasse (8), consacré au cas particulier de corps abeliens et basé sur la théorie de corps de classes locaux.

Le but du présent travail est la construction de la théorie, analogue à celle de M. Hilbert, pour les corps non-galoisiens de nombres algébriques. Pour conserver à

---

(4) *Vierteljahrschr. d. naturf. Ges. in Zürich*, 1917, pp. 67-72.

(5) *Journ. f. d. reine u. ang. Math.*, t. 149, 1919, pp. 174-188.

(6) *Acta math.* : t. 44, 1923, pp. 219-314; t. 45, 1924-1925, pp. 145-160, 303-344; t. 46, 1925, pp. 363-392; *Math. Zeitschr.*, t. 18, 1923, pp. 273-288; t. 19, 1924, pp. 276-283; t. 20, 1924, pp. 267-279; t. 25, 1926, pp. 1-8; *Math. Ann.* : t. 95, 1925, pp. 239-246; t. 96, 1926-1927, pp. 313-352; t. 97, 1926-1927, pp. 569-598; t. 99, 1928, pp. 84-117; t. 100, 1928, pp. 650-673; t. 102, 1919-1930, pp. 283-304; seuls les deux derniers mémoires des *Math. Ann.* se rapportent directement à la théorie de la ramification.

(7) *Journ. d. math. pures et appl.*, t. 96, 1931, pp. 481-498.

(8) *Journ. f. d. reine u. ang. Math.*, t. 162, 1930, pp. 169-184.

la méthode un caractère autonome j'ai voulu la développer sans me servir des résultats de la théorie de M. Hilbert pour les corps galoisiens et sans jamais procéder par extension du cas galoisien au cas général.

Antérieurement au travail actuel, Dedekind (2) avait déjà cherché à généraliser pour les corps non-galoisiens la théorie de M. Hilbert. Il l'avait fait dans les cas les plus simples (les ensembles qu'il a introduits sont des généralisations du groupe de décomposition et du groupe d'inertie), mais d'une manière peu appropriée à la nature du problème. Les notions qu'il a introduites, même convenablement généralisées aux cas supérieurs, n'ont pas de signification intrinsèque dans le corps non-galoisien étudié (sauf dans un cas, où elles coïncident avec les nôtres); elles ne permettent pas de trouver les résultats les plus importants de la théorie.

M. Ore s'est occupé aussi, dans ses mémoires de la *Mathematische Zeitschrift* et aussi dans certains de ses mémoires des *Mathematische Annalen*, des corps non-galoisiens de nombres $\mathfrak{P}$-adiques. Mais ses recherches, très intéressantes, n'ont qu'un rapport indirect avec l'objet de ce travail.

*
* *

Dans le premier chapitre de ce travail, je construis pour les corps algébriques non-galoisiens un appareil analogue à celui que fournit le groupe de Galois pour les corps galoisiens, un tel appareil étant nécessaire pour pouvoir formuler d'une manière claire et pour pouvoir démontrer, sans se servir des résultats de cas galoisiens, les résultats de la théorie de la ramification d'idéaux des corps non-galoisiens. Il est commode d'utiliser pour cela une notion introduite récemment (1934) par M. F. Marty (9) : celle de l'*hypergroupe ;* je développe un peu la théorie de M. Marty dans le cas particulier (hypergroupes de classes) qui intéresse ce travail.

Rappelons d'abord les définitions de M. Marty :

Un *hypergroupe* est un ensemble $\mathfrak{H}$ organisé par une loi de composition ab de tout $b \leqslant \mathfrak{H}$ par tout $a \leqslant \mathfrak{H}$ telle que

1° $ab < \mathfrak{H}$ et n'est pas vide;

2° $\sum_{x \leqslant ab} xc = \sum_{x \leqslant bc} ax$;

(9) *Comptes rendus du Congrès de Stockholm*, 1934, p. 45; *C. R.*, t. 201, 14 octobre 1935, pp. 636-638; *Ann. de l'Ec. norm. sup.*, t. 53, 1936, pp. 83-123.

3° a, c étant éléments quelconques de $\mathfrak{H}$, il existe $x \leqslant \mathfrak{H}$ tel que $ax \geqslant c$ et $x' \leqslant \mathfrak{H}$ tel que $x'a \geqslant c$.

$h < \mathfrak{H}$ s'appelle un *sous-hypergroupe* de $\mathfrak{H}$ s'il est un hypergroupe par rapport à la loi de composition de $\mathfrak{H}$.

Deux hypergroupes $\mathfrak{H}$ et $\mathfrak{H}'$ s'appellent *isomorphes* ($\mathfrak{H} \simeq \mathfrak{H}'$) s'il existe une correspondance biunivoque $c \rightarrow c'$ entre $\mathfrak{H}$ et $\mathfrak{H}'$ telle que pour tous $a, b \leqslant \mathfrak{H}$ on ait $(ab)' = a'b'$.

On vérifie facilement que les classes à droite (par exemple) dans un groupe G suivant un de ses sous-groupes g, composées suivant la loi de composition de G, forment un hypergroupe que M. Marty appelle l'hypergroupe *de classes* (à droite) de G suivant g, et que je désigne par $(G/g)_D$.

Cela étant, j'appelle *hypergroupe*$_D$ tout hypergroupe isomorphe à un hypergroupe de classes à droite. Je démontre que tout sous-hypergroupe d'un hypergroupe$_D$ est encore un hypergroupe$_D$. Soient $\mathfrak{H}$ un hypergroupe$_D$ et h un sous-hypergroupe de $\mathfrak{H}$. Si $c \leqslant \mathfrak{H}$, j'appelle *ch la classe de c suivant h*. Je démontre que les classes suivant h dans $\mathfrak{H}$, composées d'après la loi de composition de $\mathfrak{H}$, forment un hypergroupe$_D$, que je désigne par $(\mathfrak{H}/h)_D$ et que j'appelle *hypergroupe quotient droit* de $\mathfrak{H}$ par h. Je démontre que si $\mathfrak{H}_1$, $\mathfrak{H}_2$, h sont hypergroupes$_D$ tels que $\mathfrak{H}_1 > \mathfrak{H}_2 > h$, on a

$$(1) \qquad ((\mathfrak{H}_1/h)_D \,/\, (\mathfrak{H}_2/h)_D)_D = (\mathfrak{H}_1/\mathfrak{H}_2)_D.$$

Si h est un sous-hypergroupe d'un hypergroupe $\mathfrak{H}$, M. Marty l'appelle *invariant*, si pour tout $c \leqslant \mathfrak{H}$ on a $hc = ch$. $\mathfrak{H}$ étant un hypergroupe$_D$, j'appelle son sous-hypergroupe h *semi-invariant*, si pour tout $c \leqslant \mathfrak{H}$ on a $hc \geqq ch$.

Soit K/k un corps algébrique et $\overline{K}/k$ un de ses sous-corps. $G_{K/k}$, $G_{\overline{K}/k}$ désignant l'ensemble de tous les isomorphismes resp. de K/k, $\overline{K}/k$, soit $\sigma \leqslant G_{K/k}$. J'appelle $\bar{\sigma} \leqslant G_{\overline{K}/k}$, tel que pour tout $\bar{\alpha} \leqslant \overline{K}$ on a $\bar{\sigma}\,\bar{\alpha} = \sigma\bar{\alpha}$, *correspondant* de σ dans $\overline{K}$ (corr.$_{\overline{K}}\,\sigma$), soit $\bar{\sigma} \leqslant G_{\overline{K}/k}$. J'appelle l'ensemble de tous les $\sigma \leqslant G_{K/k}$, tels que corr.$_{\overline{K}}\sigma = \bar{\sigma}$, *l'ensemble générateur* de $\bar{\sigma}$ dans K (gen.$_K\,\bar{\sigma}$). Je donne des définitions analogues pour les ensembles des σ et des $\bar{\sigma}$.

Soit K^*/k un surcorps galoisien de K/k. La correspondance $\sigma \rightarrow$ gen.$_{K^*}\sigma$ ($\sigma \leqslant G_{K/k}$) applique d'une manière bi-univoque $G_{K/k}$ sur l'ensemble de classes à droite dans le groupe $G_{K^*/k}$ suivant son sous-groupe $G_{K^*/K}$. Si l'on organise $G_{K/k}$ par la loi de

composition telle que le composé de deux éléments de $G_{K/k}$ correspond, dans la correspondance précédente, au composé d'éléments correspondants de $(G_{K*/k}/G_{K*/K})_D$ (composés dans le même ordre), c'est-à-dire telle que, si $\sigma_1, \sigma_2 \leqslant G_{K/k}$,

$$\sigma_1\sigma_2 = \text{corr.}_K \{ \text{gen.}_{K*}\, \sigma_1 \cdot \text{gen.}_{K*}\, \sigma_2 \} \tag{2}$$

$G_{K/k}$ devient un hypergroupe$_D$ isomorphe à $(G_{K*/k}/G_{K*/K})_D$. On vérifie facilement que la loi de composition de $G_{K/k}$ ainsi organisé ne dépend pas du choix de surcorps galoisiens K^*/k de K/k. $G_{K/k}$ avec cette loi de composition s'appellera *l'hypergroupe de Galois* (ou simplement *l'hypergroupe*) de K/k.

Le théorème fondamental de la théorie de Galois peut se traduire ainsi : si $\overline{K}/k$ est un sous-corps de K/k, $G_{K/\overline{K}}$ est un sous-hypergroupe de $G_{K/k}$; si h est un sous-hypergroupe de $G_{K/k}$, il existe un et un seul sous-corps $\overline{K}/k$ de K/k tel que $h = G_{K/\overline{K}}$; $G_{\overline{K}/k} \simeq (G_{K/k}/G_{K/\overline{K}})_D$.

Soit U^* un sous-groupe de $G_{K*/k}$ et soit $U = \text{corr.}_K U^*$. Si $\sigma \leqslant U$, $\text{gen.}_{K*}\sigma \wedge U^*$ n'est pas vide et est, par conséquent, une classe à droite suivant $G_{K*/K} \wedge U^*$ dans U^*. Donc, si l'on organise U par la loi de composition, qui sera dite *induite* par U^*, donnée par

$$\sigma_1\sigma_2 = \text{corr.}_K \{ (\text{gen.}_{K*}\, \sigma_1 \wedge U^*) \cdot (\text{gen.}_{K*}\, \sigma_2 \wedge U^*) \} \qquad (\sigma_1\sigma_2 \leqslant U), \tag{3}$$

U devient un hypergroupe, qui sera désigné par $U^{(U^*)}$, isomorphe à $(U^*/(U^* \wedge G_{K*/K}))_D$. On vérifie facilement que la loi de composition de U induite par U^* ne dépend que du correspondant de U^* dans le corps de Galois de K/k.

Je démontre un certain nombre de propriétés d'hypergroupes$_D$, et de $G_{K/k}$, $U^{(U^*)}$ en particulier, qui sont nécessaires pour les démonstrations des chapitres suivants. Je n'en parle pas, parce que ces résultats ne jouent dans ce travail qu'un rôle auxiliaire.

***

Le deuxième chapitre est consacré à la construction pour les corps non-galoisiens de la théorie qui correspond à celle de M. Hilbert pour les corps galoisiens et la comprend comme un cas particulier. Voici un tableau confrontant les définitions et les résultats de ce chapitre avec les définitions et les résultats correspondants de la théorie de M. Hilbert. J'écris à droite les définitions et les résultats pour les corps non-

galoisiens et j'écris à gauche les définitions et les résultats correspondants pour les corps galoisiens. Si un résultat, une définition ou une hypothèse se formulent de la même manière pour le cas général et pour le cas galoisien, je supprime la raie verticale au milieu de la page et j'écris comme d'habitude :

Soient k un corps de nombres algébriques (de degré fini) et K

une extension galoisienne	une extension
de k (de degré fini)	
	soient K^*/k un surcorps galoisien de K/k, et $\mathfrak{P}^*$ un idéal premier de K^*
soit $\mathfrak{P}$	
un idéal premier de K	
$\mathfrak{p}$, p	
idéal correspondant de	idéaux correspondants des resp. K,
k et le premier rationnel correspondant.	
	Soit $\mathfrak{P}^{*a}$ la contribution de $\mathfrak{P}^*$ dans $\mathfrak{P}$.

L'ensemble de tous les $\sigma \leqslant G_{K/k}$ tels que

$\sigma\mathfrak{P} = \mathfrak{P}$ s'appelle *groupe*	$\sigma\mathfrak{P} \equiv 0 \pmod{\mathfrak{P}^*}$ s'appelle *ensemble*
de décomposition de	
$\mathfrak{P}$	$\mathfrak{P}^*$
dans K/k et se désigne par	
$Z_{K/k}(\mathfrak{P})$	$Z_{K/k}(\mathfrak{P}^*)$
	Je démontre que si $\sigma \leqslant Z_{K/k}(\mathfrak{P}^*)$, la contribution de $\mathfrak{P}^*$ dans $\sigma\mathfrak{P}$ est $\mathfrak{P}^{*a}$

Soit ξ une forme fondamentale de K. L'ensemble de tous les $\sigma \leqslant G_{K/k}$ tels que

$\sigma\xi \equiv \xi \pmod{\mathfrak{P}}$ s'appelle *groupe*	$\sigma\xi \equiv \xi \pmod{\mathfrak{P}^*}$ s'appelle *ensemble*

d'inertie de

$\mathfrak{P}$ | $\mathfrak{P}^*$

dans K/k et se désigne par

$T_{K/k}(\mathfrak{P})$ | $T_{K/k}(\mathfrak{P}^*)$

Je démontre que si $\sigma \leqslant T_{K/k}(\mathfrak{P}^*)$, on a $\sigma\xi \equiv \xi \pmod{\mathfrak{P}^{*a}}$

soit $\sigma \leqslant T_{K/k}(\mathfrak{P})$. L'ordre de $\sigma\xi - \xi$ pour $\mathfrak{P}$, diminué d'une unité | soit $\sigma \leqslant T_{K/k}(\mathfrak{P}^*)$. Si l'ordre en $\mathfrak{P}^*$ de $\sigma\xi - \xi$ est $w + a$, $v(\sigma; \mathfrak{P}^*) = \frac{w}{a}$

s'appelle *nombre caractéristique de σ pour*

$\mathfrak{P}$ et se désigne par $v(\sigma; \mathfrak{P})$. Soit

$$0 < v_0(K/k; \mathfrak{P}) < v_1(K/k; \mathfrak{P}) < \cdots$$
$$\cdots < v_m(K/k; \mathfrak{P}) = +\infty$$

| $\mathfrak{P}^*$. Soit

$$0 < v_0(K/k; \mathfrak{P}^*) < v_1(K/k; \mathfrak{P}^*) < \cdots$$
$$\cdots < v_m(K/k; \mathfrak{P}^*) = +\infty$$

l'ensemble de tous les nombres caractéristiques positifs distincts, rangés dans l'ordre de grandeurs croissantes, des

$\sigma \leqslant T_{K/k}(\mathfrak{P})$ pour $\mathfrak{P} \cdot v_q(K/k; \mathfrak{P})$ | $\sigma \leqslant T_{K/k}(\mathfrak{P}^*)$ pour $\mathfrak{P}^* \cdot v_q(K/k; \mathfrak{P}^*)$

($q = 0, 1, \ldots, m$) s'appelle le *q-ième nombre de ramification* de

$\mathfrak{P}$ | $\mathfrak{P}^*$

dans K/k. On pose, de plus, par convention spéciale,

$v_{-1}(K/k; \mathfrak{P}) = 0$. Le nombre de ramification $v_q(K/k; \mathfrak{P})$ | $v_{-1}(K/k; \mathfrak{P}^*) = 0$. Le nombre de ramification $v_q(K/k; \mathfrak{P}^*)$

est dit *impropre* si $q = -1$ ou $q = m$; sinon, il est dit *propre*. L'ensemble de tous les

$\sigma \leqslant T_{K/k}(\mathfrak{P})$ tels que $v(\sigma; \mathfrak{P}) \geqq v_q(K/k; \mathfrak{P})$ s'appelle *groupe* | $\sigma \leqslant T_{K/k}(\mathfrak{P}^*)$ tels que $v(\sigma; \mathfrak{P}^*) \geqq v_q(K/k; \mathfrak{P}^*)$ s'appelle *ensemble*

de ramification d'ordre q ($q = -1, 0, 1, \ldots, m$) de

$\mathfrak{P}$ | $\mathfrak{P}^*$

dans K/k et se désigne par

$\overset{(q)}{V}_{K/k}(\mathfrak{P})$. On a $T_{K/k}(\mathfrak{P}) = \overset{(-1)}{V}_{K/k}(\mathfrak{P}).\overset{(0)}{V}_{K/k}(\mathfrak{P})$

$\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$. On a $T_{K/k}(\mathfrak{P}^*) = \overset{(-1)}{V}_{K/k}(\mathfrak{P}^*).\overset{(0)}{V}_{K/k}(\mathfrak{P}^*)$

est encore appelé *l'ensemble de ramification de*

$\mathfrak{P}$ dans K/k tout court et noté $V_{K/k}(\mathfrak{P})$. On voit que

$$Z_{K/k}(\mathfrak{P}) \geqq \overset{(-1)}{V}_{K/k}(\mathfrak{P}) \geqq \overset{(0)}{V}_{K/k}(\mathfrak{P}) > \overset{(1)}{V}_{K/k}(\mathfrak{P}) > \cdots > \overset{(m)}{V}_{K/k}(\mathfrak{P}) = \{1_K\}$$

$\mathfrak{P}^*$ dans K/k tout court et noté $V_{K/k}(\mathfrak{P}^*)$. On voit que

$$Z_{K/k}(\mathfrak{P}^*) \geqq \overset{(-1)}{V}_{K/k}(\mathfrak{P}^*) \geqq \overset{(0)}{V}_{K/k}(\mathfrak{P}^*) > \overset{(1)}{V}_{K/k}(\mathfrak{P}^*) > \cdots > \overset{(m)}{V}_{K/k}(\mathfrak{P}^*) = \{1_K\}$$

où 1_K est l'isomorphisme identique de K. Désignons par

$z(K/k;\mathfrak{P}), n_q(K/k;\mathfrak{P})\ (q = -1, 0, 1, \ldots, m)$ le nombre d'éléments resp. de $Z_{K/k}(\mathfrak{P})$, $\overset{(q)}{V}_{K/k}(\mathfrak{P})$, et posons

$$r_q(K/k;\mathfrak{P}) = \frac{n_q(K/k;\mathfrak{P})}{n_{q+1}(K/k;\mathfrak{P})}\ (q = -1, 0, 1, \ldots, m-1).$$

$z(K/k;\mathfrak{P}^*), n_q(K/k;\mathfrak{P}^*)\ (q = -1, 0, 1, \ldots, m)$ le nombre d'éléments resp. de $Z_{K/k}(\mathfrak{P}^*)$, $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$, et posons

$$r_q(K/k;\mathfrak{P}^*) = \frac{n_q(K/k;\mathfrak{P}^*)}{n_{q+1}(K/k;\mathfrak{P}^*)}\ (q = -1, 0, 1, \ldots, m-1).$$

Appelons $\sigma^*\sigma$, σ^* étant dans $G_{K^*/k}$ et σ étant dans $G_{K/k}$, l'élément de $G_{K/k}$ tel que pour tout $\alpha \in K$ on a $(\sigma^*\sigma)\alpha = \sigma^*(\sigma\alpha)$. On vérifie facilement que si $\sigma^* \in G_{K^*/K}$, la correspondance $\sigma \to \sigma^*\sigma$ est un automorphisme de $G_{K/k}$. Soit $\mathfrak{P}_1^*$ un facteur premier de $\mathfrak{P}$ dans K^* autre que $\mathfrak{P}^*$. Il existe $\sigma^* \in G_{K^*/K}$ tel que $\sigma^*\mathfrak{P}^* = \mathfrak{P}_1^*$. On prouve facilement que $Z_{K/k}(\mathfrak{P}_1^*) = \sigma^* Z_{K/k}(\mathfrak{P}^*)$, $T_{K/k}(\mathfrak{P}_1^*) = \sigma^* T_{K/k}(\mathfrak{P}^*)$ et, si $\sigma \in T_{K/k}(\mathfrak{P}^*)$, $v(\sigma^*\sigma;\mathfrak{P}_1^*) = v(\sigma;\mathfrak{P}^*)$. Il en résulte qu'il existe un automorphisme de $G_{K/k}$ qui transforme la suite caractéristique de $\mathfrak{P}^*$ dans K/k dans celle de $\mathfrak{P}_1^*$ en conservant les nombres caractéristiques. En particulier,

$z(\mathrm{K}/k;\mathfrak{P}^*)$, $n_q(\mathrm{K}/k;\mathfrak{P}^*)$, $v_q(\mathrm{K}/k;\mathfrak{P}^*)$ ne dépendent pas du choix de $\mathfrak{P}^*/\mathfrak{P}$. Dès lors on peut les noter et appeler comme dans le cas galoisien, ce qui sera supposé dans la suite.

Posons

$$Z^* = Z_{K^*/K}(\mathfrak{P}^*),\ T^* = T_{K^*/K}(\mathfrak{P}^*),\ V^* = V_{K^*/k}(\mathfrak{P}^*)$$

$Z_{K/k}(\mathfrak{P}),\ \overset{(q)}{V}_{K/k}(\mathfrak{P})$ $(q = -1, 0, 1, \ldots, m)$ sont groupes.

$Z_{K/k}(\mathfrak{P}^*)^{(Z^*)},\ \overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(Z^*)}$ $(q = -1, 0, 1, \ldots, m)$ sont hypergroupes.

Il en résulte que $\dfrac{z(\mathrm{K}/k;\mathfrak{P})}{n_{-1}(\mathrm{K}/k;\mathfrak{P})}$ et tous les $r_q(\mathrm{K}/k;\mathfrak{P})$ $(q = -1, 0, 1, \ldots, m-1)$ sont entiers. Soient e, f l'ordre et le degré de $\mathfrak{P}$ dans K/k. Alors $z(\mathrm{K}/k;\mathfrak{P}) = ef$ et $n_{-1}(\mathrm{K}/k;\mathfrak{P}) = e$. Soit $\bar{n}$ la norme absolue de $\mathfrak{p}$ dans k.

Si $\sigma \leqslant Z_{K/k}(\mathfrak{P})$, il existe des entiers i tels que pour tout entier α de K on a $\sigma\alpha \equiv \alpha^{\bar{n}^i} \pmod{\mathfrak{P}}$.

Si $\sigma \leqslant Z_{K/k}(\mathfrak{P}^*)$, il existe des entiers i tels que pour tout entier α de K on a $\sigma\alpha \equiv \alpha^{\bar{n}^i} \pmod{\mathfrak{P}^*}$.

L'ensemble de tous les i ayant cette propriété est une classe d'entiers rationnels (mod f). Cette classe, qui est une fonction de σ définie dans $Z_{K/k}(\mathfrak{P})$ $(Z_{K/k}(\mathfrak{P}^*))$, sera désignée par

$$i_k(\sigma;\mathfrak{P}) \qquad | \qquad i_k(\sigma;\mathfrak{P}^*)$$

$i_k(\sigma) = 0$ équivaut à $\sigma \leqslant T_{K/k}$. On a

$$i_k(\sigma_1\sigma_2) = i_k(\sigma_1) + i_k(\sigma_2),$$

| la loi de composition étant induite par Z^*,

et $i_k(Z_{K/k})$ est l'ensemble de toutes les classes d'entiers rationnels (mod f). $\sigma \to i_k(\sigma)$ établit un isomorphisme de

$$Z_{K/k}(\mathfrak{P})/T_{K/k}(\mathfrak{P}) \qquad | \qquad (Z_{K/k}(\mathfrak{P}^*)^{(Z^*)}/T_{K/k}(\mathfrak{P}^*)^{(Z^*)})_D$$

au groupe additif de classes rationnelles (mod f).

$T_{K/k}(\mathfrak{P})$ est invariant dans $Z_{K/k}(\mathfrak{P})$
$Z_{K/k}(\mathfrak{P}) / T_{K/k}(\mathfrak{P})$

$T_{K,k}(\mathfrak{P})^{(Z^*)}$ est invariant dans $Z_{K/k}(\mathfrak{P}^*)^{(Z^*)}$
$(Z_{K/k}(\mathfrak{P}^*)^{(Z^*)} / T_{K/k}(\mathfrak{P}^*)^{(Z^*)})_D$

est un groupe cyclique d'ordre f.

Soit $\sigma \leqslant T_{K/k}(\mathfrak{P})$. On peut montrer que si π est un nombre de K d'ordre 1 en $\mathfrak{P}$, l'ordre en $\mathfrak{P}$ de $\sigma\pi - \pi$ est $1 + v(\sigma; \mathfrak{P})$.

Désignons par $\beta_{-1}(\sigma; \mathfrak{P})$ la classe de restes (mod $\mathfrak{P}$) de K qui contient $\frac{\sigma\pi}{\pi}$.

Soit $\sigma \leqslant T_{K,k}(\mathfrak{P}^*)$. On peut montrer que si π est un nombre de K d'ordre 1 en $\mathfrak{P}$, l'ordre en $\mathfrak{P}^*$ de $\sigma\pi - \pi$ est $a(1+v(\sigma; \mathfrak{P}^*))$.

Désignons par $\beta_{-1}(\sigma; \mathfrak{P}^*)$ la classe de restes (mod $\mathfrak{P}^*$) de K^* qui contient $\frac{\sigma\pi}{\pi}$.

C'est une fonction de σ, définie sur $T_{K/k}$, qui ne dépend pas du choix de π. $\beta_{-1}(\sigma) = 1$ équivaut à $\sigma \leqslant V_{K/k}$.

On trouve, si $\sigma_1, \sigma_2 \leqslant T_{K/k}(\mathfrak{P})$,

$$\beta_{-1}(\sigma_1\sigma_2; \mathfrak{P}) = \beta_{-1}(\sigma_1; \mathfrak{P}) \cdot \beta_{-1}(\sigma_2; \mathfrak{P})$$

Je montre que, la loi de composition étant induite par T^*, on a $(\sigma_1, \sigma_2 \leqslant T_{K/k}(\mathfrak{P}^*))$

$$\beta_{-1}(\sigma_1\sigma_2; \mathfrak{P}^*) = \beta_{-1}(\sigma_1; \mathfrak{P}^*) \cdot \beta_{-1}(\sigma_2; \mathfrak{P}^*)$$

Soit F le degré absolu de $\mathfrak{P}$ et, α^* désignant une classe de restes (mod $\mathfrak{P}^*$) dans K^*, soit $< \alpha^* >_F$ l'ensemble de tous les $\alpha^{*p^{iF}}$ ($i = 0, 1, \ldots$) distincts. Je démontre que, si la loi de composition est celle induite par Z^* et si $\sigma_1, \sigma_2 \leqslant T_{K/k}(\mathfrak{P}^*)$, on a

$$\beta_{-1}(\sigma_1\sigma_2; \mathfrak{P}^*) = \beta_{-1}(\sigma_1; \mathfrak{P}^*) \cdot < \beta_{-1}(\sigma_2; \mathfrak{P}^*) >_F$$

$V_{K/k}(\mathfrak{P})$ est invariant dans $T_{K/k}(\mathfrak{P})$

$V_{K/k}(\mathfrak{P}^*)^{(T^*)}$ est invariant dans $T_{K/k}(\mathfrak{P}^*)^{(T^*)}$ et $V_{K/k}(\mathfrak{P}^*)^{(Z^*)}$ est semi-invariant dans $T_{K/k}(\mathfrak{P}^*)^{(Z^*)}$.

$\beta_{-1}(T_{K/k})$, désigné encore par $M_{-1}(K/k)$, est un groupe multiplicatif de classes de restes

(mod $\mathfrak{P}$) dans K, et si h et son ordre, il est le groupe multiplicatif de toutes les

(mod $\mathfrak{P}^*$) dans K^*, et si h est son ordre, il est le groupe multiplicatif de toutes les

racines h-ièmes de l'unité (mod $\mathfrak{P}$) . h est premier à p et divise $p^{F} - 1$

racines h-ièmes de l'unité (mod $\mathfrak{P}^*$) . h est premier à p et, F° étant le degré absolu dans K° de l'idéal premier $\mathfrak{P}^\circ$ du corps de Galois K° de K par rapport à k, h divise $p^{F^\circ} - 1$.

La correspondance $\sigma \to \beta_{-1}(\sigma)$ établit un isomorphisme de

$T_{K/k}(\mathfrak{P})/V_{K/k}(\mathfrak{P})$ au groupe multiplicatif $M_{-1}(K/k; \mathfrak{P})$,

$(T_{K/k}(\mathfrak{P}^*)^{(T^*)}/V_{K/k}(\mathfrak{P}^*)^{(T^*)})_D$ au groupe multiplicatif $M_{-1}(K/k; \mathfrak{P}^*)$ et de

$$(T_{K/k}(\mathfrak{P}^*)^{(Z^*)}/V_{K/k}(\mathfrak{P}^*)^{(Z^*)})_D$$

au même ensemble organisé en hypergroupe par la loi de composition

$$ab = a \cdot < b >_F$$

$T_{K/k}(\mathfrak{P})/V_{K/k}(\mathfrak{P})$ est un groupe cyclique d'ordre $r_{-1}(K/k; \mathfrak{P}) = h$ premier à p

$(T_{K/k}(\mathfrak{P}^*)^{(T^*)}/V_{K/k}(\mathfrak{P}^*)^{(T^*)})_D$ est un groupe cyclique d'ordre $r_{-1}(K/k; \mathfrak{P}) = h$ premier à p. Il est nécessaire et suffisant pour qu'un sous-ensemble $(A/V_{K/k}(\mathfrak{P}^*)^{(Z^*)})_D$ [10] de $(T_{K/k}(\mathfrak{P}^*)^{(Z^*)}/V_{K/k}(\mathfrak{P}^*)^{(Z^*)})_D$ soit un hypergroupe que $\beta_{-1}(A; \mathfrak{P}^*)$ soit un groupe multiplicatif

soit $0 \leqq q < m$ et soit $\sigma \leqslant \overset{(q)}{V}_{K/k}(\mathfrak{P})$.

soit $0 \leqq q < m$ et soit $\sigma \leqslant \overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$. Si π' est un nombre de K^* dont l'ordre pour $\mathfrak{P}^*$ est diviseur de $av_q(K/k; \mathfrak{P}^*)$, $\beta(\sigma; \pi', \mathfrak{P})$ désigne la classe des restes (mod $\mathfrak{P}^*$) de K^* qui contient

Désignons par $\beta_q(\sigma; \pi, \mathfrak{P})$ la classe des restes (mod $\mathfrak{P}$) de K qui contient

$$\frac{\sigma\pi - \pi}{\pi^{1 + v_q(K/k; \mathfrak{P})}}.$$

$$\frac{\sigma\pi - \pi}{\pi\pi'^{uv_q(K/k; \mathfrak{P}^*)}}$$

$\beta_q(\sigma; \pi, \mathfrak{P})$ est une fonction définie sur

où u désigne le quotient de a par l'ordre

[10] A étant une réunion des classes dans un hypergroupe$_D$ K suivant un de ses sous-hypergroupes h, $(A/h)_D$ désigne l'ensemble de toutes les classes suivant h qui font partie de A. En écrivant le symbole $(A/h)_D$ on suppose implicitement que A est une réunion de classes suivant h

$\overset{(q)}{V}_{K/k}(\mathfrak{P})$ et qui se multiplie par une constante non nulle (mod $\mathfrak{P}$) quand on choisit autrement π . $\beta_q(\sigma) = 0$ équivaut à $\sigma \leqslant \overset{(q+1)}{V}_{K/k}(\mathfrak{P})$

Si $\sigma_1\sigma_2 \leqslant V_{K/k}(\mathfrak{P})$, on a

$$\beta\ (\sigma_1\sigma_2;\ \pi,\ \mathfrak{P}) = \beta_q(\sigma_1;\ \pi,\ \mathfrak{P}) + \beta_q(\sigma_2;\ \pi,\ \mathfrak{P})$$

$\overset{(q+1)}{V}_{K/k}(\mathfrak{P})$ est invariant dans $\overset{(q)}{V}_{K/k}(\mathfrak{P})$.

de π' pour $\mathfrak{P}^*$. $\beta_q(\sigma;\ \pi',\ \mathfrak{P}^*)$ est une fonction définie sur $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$ qui ne dépend pas de π employé pour la former et qui se multiplie par une constante non nulle (mod $\mathfrak{P}^*$) quand on change π' . $\beta_q(\sigma) = 0$ équivaut à $\sigma \leqslant \overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)$.

Si $\sigma_1, \sigma_2 \leqslant \overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$ et si la loi de composition est induite par V^*,

$$\beta_q(\sigma_1\sigma_2;\ \pi',\ \mathfrak{P}^*) = \beta_q(\sigma_1;\ \pi',\ \mathfrak{P}^*) + \beta_q(\sigma_2;\ \pi',\ \mathfrak{P}^*),$$

δ_q étant le dénominateur de $v_q(K/k;\ \mathfrak{P})$ mis sous forme d'une fraction irréductible, soit ε_{δ_q} l'ensemble de toutes les classes α^* (mod $\mathfrak{P}^*$) tels que $\alpha^{*\delta_q} = 1$. A étant un ensemble de classes (mod $\mathfrak{P}^*$), désignons par $[A]_{\delta_q}$ l'ensemble $A.\varepsilon_{\delta_q}$. Je démontre que si $\sigma_1,\ \sigma_2 \leqslant \overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$ et si la loi de composition est induite par T^*, on a

$$\beta_q(\sigma_1\sigma_2;\ \pi',\ \mathfrak{P}^*) = \beta_q(\sigma_1;\ \pi',\ \mathfrak{P}^*) + [\beta_q(\sigma_2;\ \pi',\ \mathfrak{P}^*)]_{\delta_q}$$

Soit γ la classe de tous les nombres α^* de K^* tels que $\pi \equiv \alpha^*\pi'^u$ (mod $\mathfrak{P}^*$) et soit $\gamma^{*a} = \gamma$. Je démontre que si la loi de composition est induite par Z^* et si σ_1, $\sigma_2 \leqslant \overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$, on a

$$\gamma^{*-av_q}\beta_q(\sigma_1\sigma_2;\ \pi',\ \mathfrak{P}^*) = \gamma^{*-av_q}\beta_q(\sigma_1;\ \pi',\ \mathfrak{P}^*) + [< \gamma^{*-av_q}\beta_q(\sigma_2;\ \pi',\ \mathfrak{P}^*) >_F]_{\delta_q}$$

$\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(V^*)}$ est invariant dans $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(V^*)}$; $\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(T^*)}$ et $\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(Z^*)}$ sont semi-invariants dans resp. $\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(T^*)}$ et $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(Z^*)}$.

$\beta_q(\overset{(q)}{V}_{K/k}(\mathfrak{P}); \pi, \mathfrak{P})$, désigné aussi par $M_q(K/k; \pi, \mathfrak{P})$,

$\beta_q(\overset{(q)}{V}_{K/k}(\mathfrak{P}^*); \pi', \mathfrak{P}^*)$, désigné aussi par $M_q(K/k; \pi', \mathfrak{P}^*)$,

est un module dans le corps fini de classes

(mod $\mathfrak{P}$) de K

(mod $\mathfrak{P}^*$) de K^*, admettant comme opérateurs la multiplication par $\varepsilon_{\delta q}$ et la transformation

$$\alpha^* \longrightarrow \gamma^{*av_q(1-p^F)}\,\alpha^{*p^F}$$

Son nombre d'éléments est une puissance de p, soit $p^{l_q}(K/k; \mathfrak{P})$. On trouve que

$$l_q(K/k; \mathfrak{P}) \leqq F. \qquad l_q(K/k; \mathfrak{P}) \leqq F^0.$$

La correspondance $\sigma \longrightarrow \beta_q(\sigma)$ établit un isomorphisme de

$\overset{(q)}{V}_{K/k}(\mathfrak{P})/\overset{(q+1)}{V}_{K/k}(\mathfrak{P})$ au module $M_q(K/k; \pi, \mathfrak{P})$

$(\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(V^*)}/\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(V^*)})_D$

au module $M_q(K/k; \pi', \mathfrak{P}^*)$, de

$(\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(T^*)}/\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(T^*)})_D$

au même ensemble organisé en hypergroupe par la loi de composition

$$ab = a + [b]_{\delta_q},$$

et de

$(\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(Z^*)}/\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(Z^*)})_D$

au même ensemble organisé en hypergroupe par la loi de composition

$$\gamma^{*-av_q} \cdot ab = \gamma^{*-av_q} \cdot a + [<\gamma^{*-av_q} \cdot b>_F]_{\delta_q}$$

$\overset{(q)}{V}_{K/k}(\mathfrak{P})/\overset{(q+1)}{V}_{K/k}(\mathfrak{P})$ est un groupe abelien du rang $l_q(K/k; \mathfrak{P})$ et du type $(p, p, \ldots, p)$

$(\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(V^*)}/\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(V^*)})_D$ est un groupe abelien du rang $l_q(K/k; \mathfrak{P})$ et du type $(p, p, \ldots, p)$. Pour qu'un sous-ensemble $(A/\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*))_D$ de

$(\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(T^*)}/\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(T^*)})_D$

soit son sous-hypergroupe, il est nécessaire et suffisant que $\beta_q(A, \pi', \mathfrak{P}^*)$ soit un module par rapport au corps fini engendré par les classes α^* (mod $\mathfrak{P}^*$) tels que $\alpha^{*\delta_q} = 1$. Pour que le même ensemble soit sous-hypergroupe de

$$(\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(Z^*)}/\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(Z^*)})_D$$

il est nécessaire et suffisant que $B_q(A;\pi',\mathfrak{P}^*)$ soit encore conservé par la transformation $\alpha^* \to \gamma^{*\, av_q(1-p^F)}\alpha^{*p^F}$

$r_q(K/k;\mathfrak{P}) = p^{i_q(K/k;\mathfrak{P})}$ est une puissance de p ($q = 0, 1, \ldots, m-1$). Si $0 \leq q < m$ et $j_q(K/k;\mathfrak{P}) = \sum_{s=q}^{m-1} l_s(K/k;\mathfrak{P})$, $n_q(K/k;\mathfrak{P}) = p^{j_q}(K/k;\mathfrak{P})$ et est, ainsi, une puissance de p. $r_{-1}(K/k;\mathfrak{P})$ est le plus grand facteur premier à p de e, et $n_0(K/k;\mathfrak{P})$ est la contribution de p dans e.

Il existe les corps K_z/k, K_q/k, appelés resp. *corps de décomposition, de ramification d'ordre* q *de* $\mathfrak{P}$ *dans* K/k

($q = -1, 0, 1, \ldots, m$) tels que resp. $G_{K/K_z} = Z_{K/k}(\mathfrak{P})$, $G_{K/K_q} = \overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$

Pour qu'il existe le corps K_z/k, K_q/k appelée resp. *corps de décomposition, de ramification d'ordre* q

($q = -1, 0, 1, \ldots, m$) de $\mathfrak{P}^*$ dans K/k, tel que resp. $G_{K/K_z} = Z_{K/k}(\mathfrak{P}^*)$, $G_{K/K_q} = \overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$ il est nécessaire et suffisant que resp. $Z_{K/k}(\mathfrak{P}^*)$, $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$ soit le même pour tous les $\mathfrak{P}^*|\mathfrak{P}$ (il sera désigné dans ce cas resp. $Z_{K/k}(\mathfrak{P})$, $\overset{(q)}{V}_{K/k}(\mathfrak{P})$).

Il résulte de ce théorème qu'on peut appeler K_z/k, K_q/k resp. corps de décomposition, de ramification d'ordre q de $\mathfrak{P}$ dans K/k

Si K_z existe,

l'idéal premier $\mathfrak{p}_z$ de K_z correspondant à $\mathfrak{P}$ est $\mathfrak{P}^e$ et son degré dans K_z/k est 1. K_z/k est le plus grand sous-corps de K/k où l'idéal premier divisible par $\mathfrak{P}$ est d'ordre et de degré 1.

| Si K_{-1} existe,

l'idéal premier $\mathfrak{p}_{-1}$ de K_{-1} correspondant à $\mathfrak{P}$ est $\mathfrak{P}^e$ et son degré dans K_{-1}/k est f. K_{-1}/k est le plus grand sous-corps de K/k dont l'idéal premier divisible par $\mathfrak{P}$ est non ramifié et le plus petit sous-corps de K/k par rapport auquel $\mathfrak{P}$ est complètement ramifié dans K.

La fin de ce chapitre est consacrée au cas de corps locaux. J'étudie d'abord, d'une manière plus précise qu'on ne le faisait avant moi, la question de correspondance entre les isomorphismes d'un corps K/k et de son corps local $K(\mathfrak{P})/k(\mathfrak{p})$. Je montre que, contrairement à ce qui semble à première vue, cette correspondance dépend du choix de l'idéal $\mathfrak{P}^*$ de K^*. J'étends en quelques mots la théorie précédente au cas local où elle subit des simplifications considérables : en particulier, dans un corps local, le corps de décomposition et les corps de ramification de tout ordre $q = -1, 0, 1, \ldots, m$ de l'idéal premier de ce corps existent toujours. Je démontre pour les corps locaux le résultat intéressant suivant : pour qu'un corps local K/k soit primitif il est nécessaire et suffisant que ou bien son degré soit un nombre premier, ou bien qu'à la fois son degré soit une puissance de p, qu'il soit complètement ramifié et n'ait qu'un seul nombre de ramification propre v et que, δ étant le dénominateur de v et f_0 étant le degré absolu dans k de son idéal premier $\mathfrak{p}$, $M_0(K/k)$ n'ait d'autre sous-module A, tel que $[<A>_{f_0}]_\delta = A$, que lui-même ou $\{0\}$. Pour finir cette partie du chapitre, je déduis un théorème sur le développement d'un $\tau\pi$ en série de puissances fractionnaires de π, π étant un nombre de K d'ordre 1 en $\mathfrak{P}$, ce théorème étant nécessaire pour une démonstration du chapitre IV.

En ce qui concerne la méthode de démonstration des résultats de ce chapitre, il est à remarquer que 1° la clé de voûte de toute la théorie est le théorème que $Z_{K/k}(\mathfrak{P}^*)^{(Z^*)}$ et les $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(Z^*)}$ sont hypergroupes; 2° cela établi, on peut suivre assez fidèlement la méthode qu'employa M. Hilbert dans le cas galoisien. Il y a toutefois une difficulté apparente pour la démonstration de ce que $z(K/k; \mathfrak{P}) = ef$ et $n_{-1}(K/k; \mathfrak{P}) = e$; M. Hilbert démontre la seconde de ces égalités, se servant du fait de l'existence du corps d'inertie dans le corps galoisien K/k, et en déduit comme conséquence la première. On ne peut pas le faire dans le cas général, mais on peut démontrer directement, et d'une manière

plus simple que celle de M. Hilbert, la première de ces égalités, en observant quelle est la contribution de $\mathfrak{P}^*$ dans $N_{K/k}(\mathfrak{P})$, et en déduire la deuxième; et il y a une difficulté réelle à justifier la possibilité d'établir dans T, V les lois de composition induites par T^*, V^* : il faut pour cela que $T_{K/k} = \text{corr.}_K T^*$ et $V_{K/k} = \text{corr.}_K V^*$. Pour cela il fallait se servir du théorème suivant de Hilbert (n° 40 de sa *Théorie de corps de nombres algébriques*), d'ailleurs nécessaire pour le chapitre III :

Si $\overline{K}/k$ est un sous-corps de K/k, ξ, $\bar{\xi}$ étant resp. les formes fondamentales de K, $\overline{K}$, $\bar{\sigma}$ étant un élément de $G_{\overline{K}/k}$, $\cdot\ \bar{\sigma}\bar{\xi} - \bar{\xi}$ et $\prod_{\sigma \leqslant \text{gen.}_K \bar{\sigma}} (\sigma\xi - \xi)$ ont le même contenu. On pouvait d'ailleurs éviter l'emploi de ce théorème au chapitre II en se servant de ce résultat de M. Hilbert : si K/k est galoisien, $n_0(K/k; \mathfrak{P})$ est une puissance de p.

*
* *

Le troisième chapitre est consacré à la question que Herbrand [7] a résolue pour le cas galoisien et que M. Hasse [11] explicita un peu plus : celle de la détermination de $Z_{\overline{K}/k}(\mathfrak{P}^*)$, des $\overset{(q)}{V}_{\overline{K}/k}(\mathfrak{P}^*)$ et des $v_q(\overline{K}/k; \mathfrak{P}^*)$ à partir du $Z_{K/k}(\mathfrak{P}^*)$, des $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$, des $v_q(K/k; \mathfrak{P}^*)$, où $\overline{K}/k$ est un sous-corps de K/k, et à un des problèmes réciproques. La méthode s'appuie sur le théorème n° 40 de Hilbert et sur certains résultats du premier chapitre. Je me borne à indiquer la résolution de cette question, la réponse à la question réciproque étant trop longue à formuler.

Soit $\overset{(q)}{\nu} = \overset{(q)}{V}_{K/k} \wedge G_{K/\overline{K}}$ et ν_q le nombre d'éléments de $\overset{(q)}{\nu}$. De même, soient $\zeta = Z_{K/k} \wedge G_{K/\overline{K}}$ et ξ son nombre d'éléments. Alors, d'abord $Z_{\overline{K}/k} = \text{corr.}_{\overline{K}} Z_{K/k}$, $z(\overline{K}/k) = \dfrac{z(K/k)}{\xi}$. Si $i_0, i_1, \ldots, i_{\mu-1}$ sont les seuls q parmi les nombres $0, 1, \ldots, m-1$ tels que $\rho_q = \dfrac{\nu_q}{\nu_{q+1}} \neq r_q(K/k)$ et si $i_{-1} = -1$ et $i_\mu = m$, on a

$$\overline{m} = \mu; \quad \overset{(q)}{V}_{\overline{K}/k} = \text{corr.}_{\overline{K}} \overset{(i_{q-1}+1)}{V}_{K/k} = \text{corr.}_{\overline{K}} \overset{(i_{q-1}+2)}{V}_{K/k} = \cdots = \text{corr.}_{\overline{K}} \overset{(i_q)}{V}_{K/k}$$

$$(4) \qquad n_q(\overline{K}/k) = \frac{n_{i_{q-1}+1}(K/k)}{\nu_{i_{q-1}+1}} = \frac{n_{i_{q-1}+2}(K/k)}{\nu_{i_{q-1}+2}} = \cdots = \frac{n_{i_q}(K/k)}{\nu_{i_q}} \quad \text{et, si} \quad \Delta_i = \frac{\nu_{-1}}{\nu_i}$$

$$(5) \qquad v_q(\overline{K}/k) = \sum_{i=0}^{i_q} \frac{v_i(K/k) - v_{i-1}(K/k)}{\Delta_i} \qquad (q = -1, 0, 1, \ldots, m).$$

Nous disons de $v_{i_q}(K/k)$ qu'il *engendre* $v_q(\overline{K}/k)$ dans K.

---

[11] La remarque finale de la note des *C. R.*, t. 197, 21 août 1933, pp. 511-512.

*
* *

Le quatrième chapitre est consacré à l'étude de dénominateurs δ_q de $v_q(K/k; \mathfrak{P})$ et à certaines autres questions qui y sont liées du point de vue de la méthode. La plus grande partie de ce chapitre est basée sur le théorème de Sylow suivant relatif aux p-groupes : tout sous-groupe d'un p-groupe fait partie d'une suite de composition de ce groupe, et sur le théorème indiqué du chapitre précédent.

Je démontre d'abord un résultat d'une importance capitale pour mon travail : δ_q est premier à p $(q = 0, 1, \ldots, m-1)$.

Je donne trois démonstrations essentiellement différentes de ce fait, dont les deux dernières sont conséquences de théorèmes plus généraux. La première démonstration est basée sur la théorie de la différente, la deuxième sur l'étude du développement d'un nombre π de $K(\mathfrak{P})$ d'ordre 1 en $\mathfrak{P}$ en série de puissances fractionnaires d'un de ses conjugués par rapport à $k(\mathfrak{p})$, la troisième sur le théorème de Sylow indiqué. Soient K^*/k un surcorps galoisien de K/k, $v^* = v_{i_q}(K^*/k; \mathfrak{P}^*)$ le nombre de ramification de $\mathfrak{P}^*$ dans K/k qui engendre $v_q(K/k; \mathfrak{P})$, et $\Delta^*_{i_q} = \Delta^{(k)}_{i_q}(K^*, K; \mathfrak{P}^*)$. Je démontre que

$$v_q(K/k; \mathfrak{P})\,\Delta^*_{i_q} \equiv v^* \ (\mathrm{mod.}\ r_{-1}(K^*/K; \mathfrak{P}^*)) \tag{6}$$

et qu'en particulier

$$\delta_q = \frac{r_{-1}(K^*/K; \mathfrak{P}^*)}{d(v^*, r_{-1}(K^*/K; \mathfrak{P}^*))}, \tag{7}$$

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

Ce résultat, avec le théorème de Sylow, sert à démontrer le théorème suivant :

Pour que tous les $v_q(K/k; \mathfrak{P})$ $(q = 0, 1, \ldots, m-1)$ soient entiers, il est nécessaire et suffisant que $T_{K^*/K}(\mathfrak{P}^*)$ fasse partie d'une suite de composition de $T_{K^*/k}(\mathfrak{P}^*)$.

Au cours de la démonstration de ce théorème, on voit que si K/k est un corps galoisien, il y a des sous-corps $K^{(\omega)}/k$ de K/k contenant K_0/k, où $\omega | r_{-1}(K/k; \mathfrak{P})$, tels que : 1° tous les $v_q(K/K^{(\omega)})$ sont divisibles par ω; 2° aucun des $v_q(K^{(\gamma)}/k)$ n'est divisible par ω; 3° il existe un sous-corps $Q^{(\omega)}/k$ de $K^{(\omega)}/k$ tel que $K^{(\omega)}/Q^{(\omega)}$ est de degré ω et complètement ramifié par rapport à $\mathfrak{P}$. Il resterait d'ailleurs à rechercher si le 3° n'est pas conséquence de 1° et 2°. J'appelle un tel $K^{(\omega)}$ ω-*corps de ramification* de K/k pour $\mathfrak{P}$.

J'ai démontré que : 1° il y a dans $T_{K/k}(\mathfrak{P})$ un élément t d'ordre $\frac{r_{-1}(K/k; \mathfrak{P})}{\omega}$ tel que $G_{K/K^{(\omega)}}$ est l'ensemble $w(t)$ de tous les $\sigma \leqslant V_{K/k}(\mathfrak{P})$ permutables avec t; 2° inversement,

si $G_{K/\overline{K}} = w(t)$, où $t \leqslant T_{K/k}(\mathfrak{P})$ est d'ordre $\frac{r_{-1}(K/k;\mathfrak{P})}{\omega}$, K est un ω-corps de ramification de K/k pour $\mathfrak{P}$; 3° tous les ω-corps de ramification de K/k pour $\mathfrak{P}$ sont conjugués entre eux par rapport à K_0.

Le même théorème de Sylow permet de démontrer l'inégalité suivante, démontrée par M. Öystein Ore ([12]) dans le cas galoisien : soit E l'ordre absolu de $\mathfrak{P}$ dans K (K/k non-galoisien) et soit $\varphi_q = n_q(K/k;\mathfrak{P})\, v_q(K/k;\mathfrak{P})$. Alors a lieu

$$\varphi_q \leqq E\frac{p}{p-1}; \tag{8}$$

si $v_q(K/k;\mathfrak{P}) \equiv 0 \pmod p$, on a $\varphi_q = E\frac{p}{p-1}$ (Égalité d'Ore) et $l_q(K/k;\mathfrak{P}) = 1$. De plus, K^* ($\mathfrak{P}^*$) contient toutes les racines p-ièmes de l'unité.

Théorème du chapitre III : le fait que les δ_q sont premiers à p et l'inégalité d'Ore permettent de donner certaines inégalités et congruences pour les nombres de ramification d'un corps qui sont conséquences d'existence des sous-corps de nature donnée dans ce corps.

Appelons *rang* d'un hypergroupe $\mathfrak{H}$ le plus petit nombre $\mathfrak{R}(\mathfrak{H})$ tel qu'il existe $\mathfrak{R}(\mathfrak{H})$ éléments de $\mathfrak{H}$ de manière que $\mathfrak{H}$ soit le seul sous-hypergroupe de $\mathfrak{H}$ qui les contient tous. Soit D le plus petit commun multiple de tous les δ_q ($q = 0, 1, \ldots, m-1$) et soit φ le p. g. c. d. de tous les $Dv_q(K/k;\mathfrak{P})$. J'ai démontré que, e_0 étant l'ordre absolu de p,

$$\mathfrak{R}(V_{K/k}(\mathfrak{P}^*)^{(Z^*)}) \leqq e_0 r_{-1}(K/k;\mathfrak{P}) \cdot F\frac{D}{\varphi}. \tag{9}$$

Je démontre un théorème qui est l'analogue du théorème de M. Ö. Ore, que si $v_0(K/k;\mathfrak{P}) \equiv 0 \pmod p$, K/k étant galoisien, $V_{K/k}(\mathfrak{P})$ est cyclique. Ce théorème est : si $v_0(K/k;\mathfrak{P}) \equiv 0 \pmod p$, $\mathfrak{R}(V_{K/k}(\mathfrak{P}^*)^{(Z^*)}) = 1$.

*
* *

Au dernier chapitre (le cinquième) je m'occupe des corps particuliers, que j'appelle *hassiens* parce que M. Hasse montra dans son travail ([8]) que les corps abeliens sont de

([12]) *Math. Annalen*, t. 102, 1929-1930, p. 000.

ce type. J'appelle un corps K/k *hassien* (ou du type $\varkappa$) pour $\mathfrak{P}$ si tous les $v_q(K/k;\mathfrak{P})$ sont entiers ($q=0, 1, \ldots, m-1$) et si, $d_q(K/k;\mathfrak{P})$ désignant $\frac{n_{-1}(K/k;\mathfrak{P})}{n_q(K/k;\mathfrak{P})}$,

$$v_q(K/k;\mathfrak{P}) \equiv v_{q-1}(K/k;\mathfrak{P}) \pmod{d_q(K/k;\mathfrak{P})}. \tag{10}$$

J'appelle un corps *du type* H' pour $\mathfrak{P}$, si l'on a seulement

$$v_q(K/k;\mathfrak{P}) \equiv v_{q-1}(K/k;\mathfrak{P}) \left(\text{mod. } \frac{d_q(K/k;\mathfrak{P})}{d_0(K/k;\mathfrak{P})}\right) \qquad (q=0,1,\ldots,m-1), \tag{11}$$

et du *type* H'' si tous les $v_q(K/k;\mathfrak{P})$ sont entiers et divisibles par $d_0(K/k;\mathfrak{P}) = r_{-1}(K/k;\mathfrak{P})$. Je donne les critères suffisants pour que K/k soit du type H, H', H'' et je montre ainsi que les corps hassiens forment une catégorie beaucoup plus étendue que les corps abeliens. Ensuite je donne le théorème suivant sur le rang de $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(Z^*)}$ du corps K/k de type H' :

$$\mathfrak{R}(V_{K/k}(\mathfrak{P}^*)^{(Z^*)}) \leqq e_0 d_0(K/k;\mathfrak{P})\, F\, \frac{D}{\varphi}\, \frac{p}{p-1} \qquad (q=0,1,\ldots,\ldots,m-1); \tag{12}$$

si G_c désigne le groupe de commutateurs de groupe G et $G^{(n)}$ désigne le groupe engendré par les puissances n-ièmes de tous les éléments de G, on a, (G_1, G_2) désignant le groupe engendré par les groupes G_1, G_2, que si K/k est de type H' pour $\mathfrak{P}$ et galoisien,

$$\left((\overset{(q)}{V}_{K/k}(\mathfrak{P}))_c,\ (\overset{(q)}{V}_{K/k}(\mathfrak{P}))^{(n)}\right) \geqq \overset{\left(q+\left[\frac{e_0 d_0(K/k;\mathfrak{P})}{\varphi}\,\frac{p}{p-1}\right]\right)}{V_{K/k}}(\mathfrak{P}). \tag{13}$$

La fin de ce chapitre est consacrée à l'étude des corps hassiens absolus, c'est-à-dire hassiens par rapport au corps rationnel. Il est inutile d'énumérer ici les résultats que j'obtiens sur ces corps. On en trouvera une grande partie dans ma deuxième note aux *Comptes rendus* de 1935.

*
* *

Ce travail se termine par deux notes. Dans la première je démontre qu'il existe effectivement des K/k et $\mathfrak{P}$ tels qu'il n'y a pas de K_z/k, c'est-à-dire tels que $Z_{K/k}(\mathfrak{P}^*)$ dépend du choix de $\mathfrak{P}^* \mid \mathfrak{P}$. Dans la deuxième je démontre l'existence des corps de type

H par rapport à k arbitraire donné pour un idéal $\mathfrak{P}$, tels que $T_{K/k}(\mathfrak{P}^*)$ et même $V_{K/k}(\mathfrak{P}^*)$ ne soient pas groupes abeliens, et même ne soient pas groupes du tout, ainsi que l'existence des corps de type H′ qui ne sont pas de type H″, et inversement.

Un grand nombre des résultats du présent travail ont été déjà indiqués par moi dans deux notes aux *Comptes rendus* de 1935 (séances du 27 mai et du 8 juillet) intitulées : *Sur la Théorie de la ramification des idéaux.*

*
* *

M. Chevalley a bien voulu s'intéresser à ce travail et m'a apporté une aide très précieuse en m'indiquant plusieurs simplifications importantes de notations et de démonstrations. Je lui adresse ici mes sincères remerciements.

Je tiens à exprimer ma profonde gratitude à l'Académie royale de Belgique, qui m'a fait l'honneur de bien vouloir insérer ce travail au Recueil de ses *Mémoires*, et tout particulièrement à MM. les Prof^rs^ Hadamard et de La Vallée Poussin.

Pour terminer, j'adresse mes respectueux remerciements à M. le Prof^r^ Montel, qui a bien voulu accepter la présidence de mon jury ; à M. le Prof^r^ Garnier, qui a bien voulu s'intéresser à ce travail, et à M. le Prof^r^ Valiron, dont la bienveillance ne m'a jamais fait défaut.

SUR LA THÉORIE
DE LA
RAMIFICATION DES IDÉAUX DE CORPS NON-GALOISIENS DE NOMBRES ALGÉBRIQUES

CHAPITRE PREMIER

HYPERGROUPES — ISOMORPHISMES DES CORPS ALGÉBRIQUES

A. — HYPERGROUPES

1° Hypergroupe. — Je me servirai d'une notion introduite récemment (1934) par M. F. Marty [1], celle d'*hypergroupe*. La définition que j'en donne est en apparence autre que celle de M. Marty, mais lui est, en fait, équivalente.

Définition 1. Un ensemble H organisé par une loi de composition de ses éléments telle que :

a) Le composé c_1c_2 de tout élément c_2 de H par tout autre élément c_1 de H soit un sous-ensemble non vide de H;

b) La loi de composition soit *associative*, c'est-à-dire

$$\sum_{c \leqslant c_1c_2} cc_3 = \sum_{c \leqslant c_2c_3} c_1c \qquad (c_1, c_2, c_3 \leqslant \mathrm{H}),$$

c) c_1c_2 étant un couple quelconque ($c_1 = c_2$ n'est pas exclu) d'éléments de H, il existe un élément c de H tel que $c_2 \leqslant c_1c$ et un élément c' de H tel que $c_2 \leqslant c'c_1$,

s'appelle un *hypergroupe*.

---

[1] Comptes rendus du Congrès de Stockholm, 1934, p. 45; *C. R.*, t. 201, 14 octobre 1935, pp. 636-638; *Ann. de l'Éc. norm. sup.*, t. 53, 1936, pp. 83-123.

Comme dans le cas de groupes, si C_1, C_2 sont deux sous-ensembles de H, on appellera composé de C_2 par C_1 la réunion de tous les c_1c_2, c_1 étant dans C_1, c_2 étant dans C_2. D'après l'associativité de la loi de composition, $(C_1C_2)\,C_3 = C_1\,(C_2C_3)$ $(C_1, C_2, C_3 < H)$.

Voici d'autres définitions de M. Marty qui seront nécessaires au cours de ce travail :

Définition 2. *Sous-hypergroupe de* H : ainsi s'appelle un sous-ensemble de H qui est lui-même hypergroupe avec la même loi de composition.

Définition 3. Sous-hypergroupe *invariant* de H : ainsi s'appelle un sous-hypergroupe C de H *permutable* avec tous les éléments c de H, c'est-à-dire tel que pour tout $c \leqslant H$ on ait

$$cC = Cc \quad (2). \tag{i}$$

Définition 4. *Unité à droite* resp. *à gauche* de H : ainsi s'appelle un élément e de H tel que pour tout élément c de H $ce = \{c\}$ resp. $ec = \{c\}$ (2).

Définition 5. Deux hypergroupes H et H′ s'appellent *isomorphes* (notation : $H \sim H'$) si l'on peut établir une correspondance biunivoque $c \rightleftarrows c'$ entre ces deux ensembles conservant la loi de composition, c'est-à-dire telle que, si $c_1 \rightleftarrows c_1'$, $c_2 \rightleftarrows c_2'$, aussi $c_1c_2 \rightleftarrows c_1'c_2'$.

La correspondance biunivoque dont il est question dans la définition 7 peut être réalisée, en général, de plusieurs manières. Chacune de ces correspondances s'appelle un *isomorphisme* de H à H′.

Si $H = H'$, un isomorphisme de H à H′ (c'est-à-dire à H) s'appelle un *automorphisme* de H.

2° Hypergroupes de classes a droite. Hypergroupes$_D$. — Soit A un ensemble organisé par une loi de composition de ses éléments telle que le composé a_1a_2 de tout $a_2 \leqslant A$ par tout $a_1 \leqslant A$ soit un sous-ensemble de A. Comme

---

(2) $\{c\}$ désigne l'ensemble formé d'un seul élément c. Plus généralement $\{a, b, \ldots\}$ désignera l'ensemble d'éléments $a, b, \ldots$

Si $c \leqslant H$ et $C < H$, on écrira souvent cC et Cc au lieu de $\{c\}C$ et (resp.) $C\{c\}$.

précédemment, A_1, A_2 étant sous-ensembles de A, A_1A_2, désigne $\sum_{a_1 \leqslant A_1,\, a_1 \leqslant A_2} a_1 a_2$ et s'appelle le composé de A_2 par A_1.

Soit que dans A est établie une relation de classification telle que le composé $\mathfrak{A}_1\mathfrak{A}_2$ de deux classes quelconques $\mathfrak{A}_1$, $\mathfrak{A}_2$ dans A est une réunion de classes. Alors on peut organiser l'ensemble $\mathfrak{A}$ de toutes les classes dans A par la loi de composition suivante : Le composé d'un $\mathfrak{A}_2 \leqslant \mathfrak{A}$ par un $\mathfrak{A}_1 \leqslant \mathfrak{A}$ est l'ensemble de toutes les classes contenues dans le composé $\mathfrak{A}_1\mathfrak{A}_2$ dans le sens de la loi de composition de A. L'ensemble A et l'ensemble $\mathfrak{A}$ ainsi organisé seront dits avoir la *même* loi de composition. Si A' est un élément d'une famille de sous-ensembles, disjoints deux à deux, de A, et $\mathfrak{A}'$ est un élément d'une famille de sous-ensembles, disjoints deux à deux, de $\mathfrak{A}$, A' et $\mathfrak{A}'$ seront considérés comme identiques si A est la réunion de toutes les classes dans A qui sont éléments de $\mathfrak{A}'$ et l'on dira par extension de la définition précédente que la loi de composition de deux ensembles A et Q est la même s'il existe une chaîne B, C, ..., P d'ensembles tels que la loi de composition est la même dans le sens précédent dans A et B, dans B et C, dans C et ..., ..., dans P et Q. On vérifie facilement que cette manière de parler ne peut pas conduire à une contradiction.

Il est évident que si une loi de composition est associative dans A, la même loi de composition est encore associative dans $\mathfrak{A}$ (supposant que $\mathfrak{A}$ peut être organisé par cette même loi).

Ceci posé, soient G un groupe et g un sous-groupe de G. Le composé de deux classes à droite $g_1 = a_1 g$ et $g_2 = a_2 g$ $(a_1, a_2 \leqslant G)$ suivant g dans G est encore la réunion $a_1 g a_2 g$ de telles classes. Donc l'ensemble de toutes les classes (à droite) suivant g dans G peut être organisé par la même loi de composition que celle de G. Montrons que cet ensemble ainsi organisé est un hypergroupe.

Il suffit de démontrer pour cela que : 1° g_1, g_2 étant deux éléments de cet ensemble, $g_1 g_2$ n'est pas vide; 2° g_1, g_2 étant deux éléments de cet ensemble, il existe un élément g_0 et un élément g_0' de cet ensemble tels que $g_1 g_0 \geqslant g_2$ et $g_0' g_1 \geqslant g_2$, le reste étant la conséquence de généralités qui précèdent. Or, 1° et 2° expriment les propriétés bien classiques de classes (à droite) dans un groupe.

Définition 6. L'hypergroupe qu'on vient d'introduire s'appellera *l'hypergroupe de classes à droite suivant g dans* G et sera désigné par $(G/g)_D$.

Soient $\mathfrak{A}$ un sous-ensemble de $(G/g)_D$ et A la réunion de toutes les classes dans G qui sont éléments de $\mathfrak{A}$. On désignera $\mathfrak{A}$ encore par le symbole $(A/g)_D$. A remarquer que quand on écrit le symbole $(A/g)_D$ on pose comme hypothèse que A est une réunion de classes (à droite) suivant g.

Théorème 1. Condition nécessaire et suffisante pour que $(A/g)_D$ soit un sous-hypergroupe de $(G/g)_D$ est que A soit un sous-groupe de G.

Démonstration. Si A est un sous-groupe de G, $(A/g)_D$ est, d'après ce qui précède, un hypergroupe avec la même loi de composition que $(G/g)_D$. Inversement, soit que $(A/g)_D$ est un sous-hypergroupe de $(G/g)_D$. Alors $(A/g)_D = (A/g)_D \cdot (A/g)_D = (AA/g)_D$, c'est-à-dire $AA = A$, et, si $ag < A$, on a d'abord que $(agA/g)_D = (ag/g)_D (A/g)_D \geqslant (ag/g)_D$, c'est-à-dire $agA \geqq ag$. Il en résulte que $A \geqslant I$, I étant l'unité de groupe G, et que $(A/g)_D \geqslant g$. Donc $a \leqslant A$ et $ag < A$ signifient la même chose et $A = AA \geqq gA$. Il en résulte que $(aA/g)_D \geqq (agA/g)_D = (ag/g)_D \cdot (A/g)_D \geqslant g$, c'est-à-dire $aA \geqq g \geqslant I$ et $A \geqslant a^{-1}$. A est un groupe. C. Q. F. D.

Conséquence 1. Si le groupe G a un nombre fini d'éléments, l'égalité $\mathfrak{A}\mathfrak{A} = \mathfrak{A}$ est nécessaire et suffisante pour qu'un $\mathfrak{A} \leqq (G/g)_D$ soit un hypergroupe de $(G/g)_D$.

Démonstration. En effet, si $\mathfrak{A} = (A/g)_D$, l'égalité $\mathfrak{A}\mathfrak{A} = \mathfrak{A}$ équivaut à $AA = A$ et cette dernière égalité est justement la condition nécessaire et suffisante pour que A soit un groupe quand G est d'ordre fini.

Théorème 2. $(G/g)_D$ est un groupe si g est un sous-groupe invariant de G et dans ce cas seulement.

Démonstration. Si g est invariant dans G, $(G/g)_D$ est évidemment le groupe quotient de G par g; soit, inversement, que $(G/g)_D$ est un groupe. Alors, si $a \leqslant G$, gag doit être une classe (à droite) suivant g. Donc, puisque $gag \geqq ag$, on doit avoir $gag = ag = agg$, c'est-à-dire $ga = ag$ et g est invariant dans G.

Définition 7. Si $\mathfrak{A}$ est un sous-hypergroupe de $(G/g)_D$ et $c \leqslant (G/g)_D$, l'ensemble $c\mathfrak{A}$ s'appelle la classe à droite de c suivant $\mathfrak{A}$ dans $(G/g)_D$.

Si pour tout $c \leqslant (G/g)_D$ on a $\mathfrak{A}c \geqq c\mathfrak{A}$, $\mathfrak{A}$ s'appelle sous-hypergroupe *semi-invariant* de $(G/g)_D$.

Théorème 3. Si $\mathfrak{A} = (A/g)_D$ est un sous-hypergroupe de $(G/g)_D$ et si $a \leqslant c \leqslant (G/g)_D$, on a

$$c\mathfrak{A} = (aA/g)_D. \tag{2}$$

Démonstration. A est un groupe et g est un sous-groupe de A. Donc

$$c\mathfrak{A} = (ag/g)_D\,(A/g)_D = (agA/g)_D = (aA/g)_D. \qquad \text{C. Q. F. D.}$$

Donc la réunion de classes dans G qui sont éléments d'une classe dans $(G/g)_D$ suivant $\mathfrak{A} = (A/g)_D$ est une classe suivant A dans G. Il en résulte, en vertu des propriétés classiques des classes (à droite) dans un groupe, que

1° Les classes de la définition 7 sont classes au sens de la théorie des ensembles, c'est-à-dire deux classes ou bien coïncident, ou bien sont disjointes;

2° Une classe est la classe de tout élément qu'elle contient et contient tous les éléments dont elle est la classe;

3° Toutes les classes suivant $\mathfrak{A}$ dans $(G/g)_D$ ont le même nombre d'éléments égal à celui de $\mathfrak{A}$, c'est-à-dire, si $\mathfrak{A} = (A/g)_D$, à l'indice de g dans A. Le nombre d'éléments de $(G/g)_D$ est multiple de celui de $\mathfrak{A}$.

Théorème 4. L'ensemble de classes à droite dans $(G/g)_D$ suivant un sous-hypergroupe $h = (A/g)_D$ de $\mathfrak{H} = (G/g)_D$ organisé par la même loi de composition que celui de $(G/g)_D$ est un hypergroupe, désigné par $(\mathfrak{H}/h)_D$ et appelé *l'hypergroupe de classes à droite suivant* h *dans* $\mathfrak{H}$ ou, mieux, *l'hypergroupe quotient à droite de* $\mathfrak{H}$ *par* h; $(\mathfrak{H}/h)_D = (G/A)_D$.

Démonstration. En vertu du théorème 3 les éléments de $(\mathfrak{H}/h)_D$ doivent être considérés comme identiques à ceux de $(G/A)_D$ dans la manière de parler dont il était convenu au commencement de ce paragraphe. Avec la même manière de parler, la loi de composition est la même dans $(\mathfrak{H}/h)_D$ et $\mathfrak{H} = (G/g)_D$ et est la même dans $(G/g)_D$ et dans G. Donc elle est la même dans $(\mathfrak{H}/h)_D$ et dans G, ce qui démontre le théorème. Comme précédemment, si $\mathfrak{A}$ est un sous-ensemble de $(\mathfrak{H}/h)_D$ et A est la réunion de toutes les classes dans $\mathfrak{H}$ qui sont éléments de A, $\mathfrak{A}$ sera noté $(A/h)_D$.

Théorème 5. La condition nécessaire et suffisante pour que $(A/h)_D$ soit un sous-hypergroupe de $(\mathfrak{H}/h)_D$, où $\mathfrak{H}$ est un hypergroupe de classes à droite, est que A soit un sous-hypergroupe de $\mathfrak{H}$.

Démonstration. Soient $\mathfrak{H} = (G/g)_D$, $h = (g_0/g)_D$ et $A = (B/g)_D$. On a, d'après le théorème 4, que $(\mathfrak{H}/h)_D = (G/g_0)_D$ et $(A/h)_D = (B/g_0)_D$. Pour que $(A/h)_D$ soit un sous-hypergroupe de $(\mathfrak{H}/h)_D$ il faut et il suffit, d'après le théorème 1, que B soit un sous-groupe de G. Mais c'est aussi la condition nécessaire et suffisante pour que A soit un sous-hypergroupe de $\mathfrak{H}$. C. Q. F. D.

Théorème 6 (Loi d'isomorphisme). Si $\mathfrak{H}$ est un hypergroupe de classes et h', h sont deux sous-hypergroupes de $\mathfrak{H}$ tels que $h' > h$, on a

$$((\mathfrak{H}/h)_D / (h'/h)_D)_D = (\mathfrak{H}/h')_D. \tag{3}$$

Démonstration. Soit que

$$\mathfrak{H} = (G/g)_D, \quad h' = (g'_0/g)_D, \quad h = (g_0/g)_D,$$

où G est un groupe. Alors g'_0, g_0, g sont sous-groupes de G et $g'_0 > g_0 > g$. On a

$$(\mathfrak{H}/h)_D = (G/g_0)_D, \quad (h'/h)_D = (g'_0/g_0)_D;$$

donc

$$((\mathfrak{H}/h)_D / (h'/h)_D)_D = (G/g'_0)_D = (\mathfrak{H}/h')_D. \qquad \text{C. Q. F. D.}$$

Théorème 7. Si h_1, h_2 sont deux sous-hypergroupes d'un hypergroupe de classes à droite $\mathfrak{H}$: 1° $h_1 \wedge h_2$ est un sous-hypergroupe de $\mathfrak{H}$; 2° si $c \leqslant \mathfrak{H}$, $ch_1 \wedge ch_2 = c(h_1 \wedge h_2)$.

Démonstration. Soit que

$$\mathfrak{H} = (G/g)_D, \quad h_1 = (g_1/g)_D, \quad h_2 (g_2/g)_D,$$

où G est un groupe. g_1, g_2 sont sous-groupes de G, donc $g_1 \wedge g_2$ est groupe et

$$h_1 \wedge h_2 = (g_1/g)_D \wedge (g_2/g)_D = ((g_1 \wedge g_2)/g)_D$$

est un hypergroupe, ce qui démontre 1°. Soit $c = (ag/g)_D$. Alors

$$ch_1 = (ag_1/g)_D, \quad ch_2 = (ag_2/g)$$

et

$$ch_1 \wedge ch_2 = (ag_1/g)_D \wedge (ag_2/g)_D = ((ag_1 \wedge ag_2)/g)_D = (a(g_1 \wedge g_2)/g)_D = c(h_1 \wedge h_2),$$

parce que g_1 et g_2 sont groupes, ce qui démontre 2°. C. Q. F. D.

Conséquence 2. En particulier, $ch_1 \wedge h_2$ est où bien vide, où bien une classe à droite suivant $h_1 \wedge h_2$. Le nombre d'éléments de $ch_1 \wedge h_2$ est 0 ou le même que celui de $h_1 \wedge h_2$.

Démonstration. Si $ch_1 \wedge h_2$ n'est pas vide, soit $c' \leqslant ch_1 \wedge h_2$. On a $ch = c'h$ et $h_2 = c'h_2$, d'où $ch_1 \wedge h_2 = c'h_1 \wedge c'h_2 = c'(h_1 \wedge h_2)$. C. Q. F. D.

Théorème 8. Si h_1, h_2 sont deux sous-hypergroupes d'un hypergroupe de classes à droite $\mathfrak{H}$, le nombre d'éléments de $(h_1h_2/h_2)_D$ est égal à celui de $(h_1/(h_1 \wedge h_2))_D$.

Démonstration. Le nombre d'éléments de $(h_1h_2/h_2)_D$ est égal au nombre de classes à droite suivant h_2 contenues dans h_1h_2, c'est-à-dire ayant une intersection non-vide avec h_1. Or, une intersection non-vide d'une classe suivant h_2 avec h_1 est une classe à droite suivant $h_1 \wedge h_2$, ce qui démontre la proposition.

Définition 8. Un hypergroupe $\mathfrak{H}$ isomorphe à un hypergroupe $(G/g)_D$ de classes à droite s'appelle un *hypergroupe*$_D$ (hypergroupe *droit*).

Si $(G/g)_D \simeq \mathfrak{H}$ peut être pris de manière que G soit d'ordre fini, $\mathfrak{H}$ sera dit un hypergroupe$_D$ *fini*.

Toutes les propriétés intrinsèques, c'est-à-dire ne faisant intervenir que les éléments et la loi de composition de l'hypergroupe regardé, des hypergroupes de classes à droite, restent, manifestement, vraies pour les hypergroupes$_D$. Les définitions de la classe à droite suivant un sous-hypergroupe et du groupe quotient droit, ainsi que celle de la semi-invariance, s'étendent aux hypergroupes$_D$ sans changer un mot.

En particulier, le théorème 1 se formule ainsi : tout sous-hypergroupe d'un hypergroupe$_D$ est un hypergroupe$_D$. Quant aux autres théorèmes on n'a qu'à y remplacer l'expression « hypergroupe de classes à droite » par celle d' « hypergronpe$_D$ » et, parfois, le signe $=$ par le signe $\simeq$.

Remarque. Les seuls hypergroupes dont il s'agira dans la suite de ce travail seront hypergroupes$_D$. Pour cette cause on supprimera toujours les termes « droit », « à droite », et l'indice $_{«D»}$ dans les énoncés et dans les démonstrations.

B. — HYPERGROUPES D'ISOMORPHISMES DES CORPS ALGÉBRIQUES

1° Notation. — Dans cette partie B du chapitre I ainsi que dans tous les chapitres suivants on employera la notation et l'on fera les conventions suivantes :

k désignera un corps de base.

Les surcorps algébriques de k (qui seront toujours supposés de degré fini par rapport à k) seront notés par la lettre K accompagnée ou non de signes (par exemple K, $\overline{K}$, K', K*, K_i).

Avec M. Hasse, au lieu de dire qu'il s'agit d'une propriété dans K par rapport à un de ses sous-corps $\overline{K}$, on dira qu'il s'agit de cette propriété *dans* $K/\overline{K}$.

Il s'agira presque toujours des propriétés par rapport à un corps k qui restera le même au cours d'un chapitre. Pour cette cause on n'indiquera jamais dans les démonstrations et dans les énoncés le corps par rapport auquel est prise une propriété quand ce corps est k, une exception à cette règle étant faite pour les seuls cas des définitions où k intervient d'une manière essentielle. Donc, l'absence de toute indication sur le corps, par rapport auquel une propriété est prise, signifie qu'il s'agit d'une propriété par rapport à k.

Les isomorphismes d'un corps désigné par la lettre K surmontée ou non de signes seront désignés par la lettre σ surmontée des mêmes signes et, éventuellement, accompagnée d'indice (par exemple les isomorphismes de $\overline{K}$ seront notés $\overline{\sigma}_1$, $\overline{\sigma}_2$, etc.) (3).

L'isomorphisme identique d'un corps K sera noté 1_K.

L'ensemble de tous les isomorphismes d'un corps algébrique $K/\overline{K}$ sera noté $G_{K/\overline{K}}$. On dira que $\overline{K}$ *appartient* dans K à $G_{K/\overline{K}}$.

---

(3) J'ai arrangé les notations des chapitres suivants de manière que les isomorphismes des corps notés K_i ne soient jamais employés au cours de ce travail.

Si $K \geqq \overline{K} \geqq \overline{\overline{K}}$, les symboles $K/\overline{K}$ et $(K/\overline{\overline{K}})/(\overline{K}/\overline{\overline{K}})$ doivent signifier la même chose. Je dois ajouter à cela encore deux conventions d'un caractère général :

1° Si dans tous les symboles d'une même nature, employés au cours d'une démonstration, un objet qui entre dans l'expression de ces symboles reste toujours le même, et s'il est clair, d'après l'énoncé, quel est cet objet, on supprimera cet objet dans l'expression de tous ces symboles.

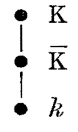
Par contre, on ne fera une telle suppression dans les symboles employés dans les énoncés qu'en vertu des conventions explicitement formulées, analogues à celle pour k.

2° Si λ est une fonction, transformation, correspondance, etc., qui fait correspondre à un objet a un objet b ou un ensemble B ($\lambda(a) = b$ resp. B) et si A est un ensemble d'objets a pour lesquels $\lambda(a)$ est défini, $\lambda(A)$ désignera l'ensemble resp. la réunion de tous les $\lambda(a)$, $a \leqslant A$.

Si Λ est un ensemble de transformations λ tel que $\lambda(a)$ est défini par tout $a \leqslant A$, $\Lambda(A)$ désignera l'ensemble (si les $\lambda(A)$ sont éléments) ou resp. la réunion (si les $\lambda(A)$ sont ensembles) de tous les $\lambda(A)$, $\lambda \leqslant \Lambda$.

Au cours de cette partie B du chapitre I seulement, α surmontée ou non de signes désignera l'élément arbitraire du corps désigné par K surmonté des mêmes signes (par exemple $\bar{\alpha}$ désigne un élément arbitraire de $\overline{K}$).

2° Correspondants et ensembles générateurs. — Soient K un corps algébrique, $\overline{K}$ un sous-corps de K :



La théorie de Galois montre que tout isomorphisme de K appliqué aux éléments de $\overline{K}$ produit un isomorphisme de $\overline{K}$ et que tout isomorphisme de $\overline{K}$ peut s'obtenir de cette manière. Ceci nous permet de poser les définitions suivantes :

Définition 1. $\bar{\sigma}$ s'appelle *correspondant* (dans $\overline{K}$) de σ, si $\bar{\sigma}\bar{\alpha} = \sigma\bar{\alpha}$ (notation : $\bar{\sigma} = \mathrm{corr}._{\overline{K}}\,\sigma$).

Définition 2. L'ensemble A de tous les σ tels que $\text{corr.}_{\overline{K}}\,\sigma = \overline{\sigma}$ s'appelle *l'ensemble générateur* (ou simplement *générateur*) de $\overline{\sigma}$ dans K (notation : $A = \text{gen.}_K\,\overline{\sigma}$).

Définition 2*a*. Si U est un ensemble de σ tel que $\text{corr.}_{\overline{K}}\,U \geqslant \overline{\sigma}$ (ce qui sera noté $U \succ \overline{\sigma}$), $\text{gen.}_K\,\overline{\sigma} \wedge U$ sera désigné par $\text{gen.}_U\,\overline{\sigma}$ et appelé *l'ensemble générateur de* σ *dans* U.

Les définitions de $\text{corr.}_{\overline{K}}$, gen._K, gen._U et de $\succ$ seront étendues aux ensembles de σ et de $\overline{\sigma}$, comme cela a été indiqué dans 1°.

Si $K > \overline{K} > \overline{\overline{K}}$, d'après les définitions précédentes on a

$$\text{corr.}_{\overline{\overline{K}}}\,A = \text{corr.}_{\overline{\overline{K}}}\,\text{corr.}_{\overline{K}}\,A \qquad (A < G_K), \tag{1}$$

$$\text{gen.}_U\,\overline{\overline{A}} = \text{gen.}_U\,\text{gen.}_{\text{corr.}_{\overline{K}}U}\,\overline{\overline{A}} \qquad (\overline{\overline{A}} < G_{\overline{\overline{K}}}), \tag{2}$$

et, en particulier,

$$\text{gen.}_K\,\overline{\overline{A}} = \text{gen.}_K\,\text{gen.}_{\overline{K}}\,\overline{\overline{A}}. \tag{3}$$

Il est évident que

$$\text{corr.}_{\overline{K}}\,\text{gen.}_U\,\overline{A} = \overline{A} \qquad (\overline{A} < G_{\overline{K}}), \tag{4}$$

$$G_{K/\overline{K}} = \text{gen.}_K\,1_{\overline{K}}. \tag{5}$$

3° Hypergroupe de K. — Considérons un corps K et une extension galoisienne K^* de K. La correspondance $\sigma^* \to \text{corr.}_K\,\sigma^*$ fait correspondre un même σ à tous les éléments d'une même classe à droite suivant $G_{K^*/K}$, et à ces éléments seulement. Donc, cette correspondance applique d'une manière biunivoque $(G_{K^*}/G_{K^*/K})_D$ sur G_K. Si, de plus, on organise G_K par la loi de composition telle que $\sigma_1\sigma_2$ soit le correspondant dans K du composé de classes suivant $G_{K^*/K}$ auxquelles correspondent σ_1, σ_2, c'est-à-dire

$$\sigma_1\sigma_2 = \text{corr.}_K\,\{\,\text{gen.}_{K^*}\,\sigma_1 \cdot \text{gen.}_{K^*}\,\sigma_2\,\} \tag{6}$$

G_K devient un hypergroupe$_D$ isomorphe à $(G_{K^*}/G_{K^*/K})_D$.

Définition 3. L'hypergroupe$_D$ précédemment défini s'appelle *l'hypergroupe de* K/*k* (4).

(4) Ou *l'hypergroupe de Galois de* K/*k*.

Il est visible que l'hypergroupe de K *ne dépend pas du choix du* K^* *employé pour le définir.* G_K *est groupe si* K *est galoisien et dans ce cas seulement* (théorème 2 de A). G_K a une et une seule unité à droite : c'est 1_K.

Il suit du théorème 1 de A que *la condition nécessaire et suffisante pour qu'un ensemble* A *des* σ *soit un sous-hypergroupe de* G_K *est que* gen._{K*} A *soit un groupe d'automorphismes de* K^*.

Or, si gen._{K*} A est un surgroupe de $G_{K*/K}$, il existe un sous-corps $\overline{K}$ de K tel que $G_{K*/\overline{K}} = \text{gen.}_{K*}$ A et inversement. Mais alors

$$A = \text{corr.}_K \text{gen.}_{K*} A = \text{corr.}_K G_{K*/\overline{K}} = G_{K/\overline{K}}. \tag{7}$$

Ce résultat montre que le théorème fondamental de la théorie de Galois peut s'exprimer ainsi :

Chaque sous-corps $\overline{K}$ *de* K *appartient à un sous-hypergroupe de* G_K; *à chaque sous-hypergroupe* A *de* G_K *appartient un sous-corps* $\overline{K}$ *de* K.

On a, si $\overline{K}$ est un sous-corps de K,

$$(G_K / G_{K/\overline{K}})_D \simeq ((G_{K*} / G_{K*/K})_D / (G_{K*/\overline{K}} / G_{K*/K})_D)_D = (G_{K*} / G_{K/*\overline{K}})_D \simeq G_{\overline{K}}. \tag{8}$$

Donc, $G_{\overline{K}}$ *est isomorphe à l'hypergroupe quotient de* G_K *par* $G_{K/\overline{K}}$. Comme le premier isomorphisme de (8) est réalisé par $\sigma^* \to \text{corr.}_K \sigma^*$, et le deuxième par $\sigma^* \to \text{corr.}_{\overline{K}} \sigma^*$, *l'isomorphisme* $(G_K/G_{K/\overline{K}})_D \simeq G_{\overline{K}}$ *se réalise par* $\sigma \to \text{corr.}_{\overline{K}} \sigma$.

Donc, *les classes suivant* $G_{K/\overline{K}}$ *dans* G_K *sont les ensembles générateurs des* $\bar{\sigma}$.

Introduisons un nouveau symbole $\sigma^*\sigma$ qui sera utile dans la suite du travail : c'est un isomorphisme de K défini par

$$(\sigma^* \sigma)\, \alpha = \sigma^* (\sigma \alpha), \tag{9}$$

c'est-à-dire

$$\sigma^* \sigma = \text{corr.}_K \{ \sigma^* \cdot \text{gen.}_{K*} \sigma \}, \tag{10}$$

Si C est une classe suivant $G_{K/\overline{K}}$ et si $\text{corr.}_{\overline{K}} C = \bar{\sigma}$, on a

$$\sigma^* C = \text{corr.}_K \{ \sigma^* \cdot \text{gen.}_{K*} C \} = \text{corr.}_K \{ \sigma^* \cdot \text{gen.}_{K*} \bar{\sigma} \} = \text{gen.}_K (\sigma^* \bar{\sigma}).$$

Soient α un élément de K et $F(\sigma_i \alpha)$ une fonction symétrique des transformés

de α par tous les éléments σ_i d'un sous-hypergroupe $A = G_{K/\overline{K}}$ de G_K. Si $\sigma \leqslant G_K$ et $\sigma^* \leqslant \text{gen.}_{K*}\,\sigma$, on a que

$$\sigma F(\sigma_i\alpha) = \sigma^* F(\sigma_i\alpha) = F(\sigma^*(\sigma_i\alpha)) = F(\sigma^*\sigma_i \cdot \alpha)$$

est la même fonction symétrique des transformés de α par les éléments de

$$\sigma^* G_{K/\overline{K}} = \text{gen.}_K(\sigma^* \cdot 1_{\overline{K}}) = \text{gen.}_K \text{corr.}_{\overline{K}}\,\sigma^* = \sigma\, G_{K/\overline{K}}.$$

4° Lois de composition induites. — Soit U^* un groupe d'automorphismes de K^* et soit $U = \text{corr.}_K U^*$. Il existe une correspondance biunivoque entre les éléments σ de U et les éléments de $(U^*/(U^* \vee G_{K*/K}))_D$ réalisée par $\sigma \to \text{gen.}_{U*}\sigma$. Cette correspondance bi-univoque permet d'organiser U en hypergroupe$_D$ d'une manière analogue à ce qui était fait dans 4° pour G_K. La loi de composition sera donc

$$\sigma_1\sigma_2 = \text{corr.}_K\{\text{gen.}_{U*}\,\sigma_1 \cdot \text{gen.}_{U*}\,\sigma_2\} \qquad (\sigma_1, \sigma_2 \leqslant U)$$

et s'appellera la loi de composition *induite* dans U par celle de U^*. L'hypergroupe ainsi obtenu sera désigné, s'il y a lieu, par $U^{(U*)}$; si W est l'un de ses sous-hypergroupes, on le désignera par $W^{(U*)}$ si l'on veut rappeler l'origine de la loi de composition qu'on y considère. L'hypergroupe quotient de U par W sera désigné par $(U/W)^{(U*)}$.

Soient $\overline{K}$ un sous-corps de K et $\bar{\sigma}$ un isomorphisme de $\overline{K}$ tel que $U \succ \bar{\sigma}$. Alors

$$\text{gen.}_U\,\bar{\sigma} = \text{corr.}_K \text{gen.}_{U*}\,\bar{\sigma} = \text{corr.}_K\{\text{gen.}_{K*}\,\bar{\sigma} \wedge U^*\}.$$

Comme $\text{gen.}_{K*}\,\bar{\sigma}$ est une classe à droite suivant $G_{K*/\overline{K}}$, $\text{gen.}_{K*}\,\bar{\sigma} \wedge U^*$ est une classe à droite suivant $G_{K*/\overline{K}} \wedge U^* = \text{gen.}_{U*}\,1_{\overline{K}}$ qui est un groupe. Donc, d'après le théorème 1 de A, $\text{corr.}_K \text{gen.}_{U*}\,1_{\overline{K}} = \text{gen.}_U\,1_{\overline{K}} = G_{K/\overline{K}} \wedge U$ *est un sous-hypergroupe de* $U^{(U*)}$ et $\text{gen.}_U\,\bar{\sigma} = \text{corr.}_K(\text{gen.}_{K*}\,\bar{\sigma} \wedge U^*)$ *est une classe à droite suivant* $G_{K/\overline{K}} \wedge U$.

Il en résulte que si A est un sous-hypergroupe de $U^{(U*)}$, *le nombre d'éléments de* $\text{corr.}_{\overline{K}} A$ (c'est-à-dire le nombre de classes suivant $\text{gen.}_U\,1_{\overline{K}}$ qui ont une intersection non vide avec A) *est égal* à celui de $(A\,\text{gen.}_U\,1_{\overline{K}}/\text{gen.}_U\,1_{\overline{K}})^{(U*)}$, donc à celui (théorème 8 de A) de

$$(A/(A \wedge \text{gen.}_U\,1_{\overline{K}}))^{(U*)} = (A/(A \wedge G_{K/\overline{K}} \wedge U))^{(U*)} = (A/(A \wedge G_{K/\overline{K}}))^{(U*)},$$

c'est-à-dire *au quotient du nombre d'éléments de* A *par celui de* $A \wedge G_{K/\overline{K}}$.

Remarque 1. Il est facile de montrer que la loi de composition dans U induite par U^* ne dépend que du correspondant de U^* dans le corps de Galois K· de K.

Remarque 2. Il est évident, d'après la conséquence 1 du théorème 1 de A, que si un ensemble W de σ est un hypergroupe par rapport à la loi de composition induite par U^* et si U_1^* est un sous-groupe de U^* tel que $\text{corr.}_K U_1^* \geqq W$: 1° W est un hypergroupe par rapport à la loi de composition induite par U_1^* ; 2° le composé de deux éléments $\sigma_1\sigma_2$ de W d'après la loi de composition induite par U_1^* est contenu dans le composé de mêmes éléments d'après la loi de composition induite par U^*.

CHAPITRE II

ENSEMBLES DE DÉCOMPOSITION, D'INERTIE ET DE RAMIFICATION

A. — CORPS DE NOMBRES ALGÉBRIQUES

Dans cette partie A du chapitre II le corps de base k sera supposé être un corps de nombres algébriques (de degré fini). K étant une extension finie de k, on désignera par K^* une extension galoisienne de k contenant K.

Soient $\mathfrak{p}$ un idéal premier de k, divisant un premier rationnel p; $\mathfrak{P}$ un diviseur premier de $\mathfrak{p}$ dans K; $\mathfrak{P}^*$ un diviseur premier de $\mathfrak{P}$ dans K^*. Soit $\mathfrak{P}^{*a}$ la contribution de $\mathfrak{P}^*$ dans $\mathfrak{P}$. Nous allons montrer qu'on peut attacher à $\mathfrak{P}^*$ une suite de sous-ensembles de l'hypergroupe de Galois de K/k qui généralise la suite définie par *Hilbert* [1] dans le cas où $K = K^*$.

Soit $(\alpha_1, \alpha_2, \ldots, \alpha_N)$ une base minima de l'anneau des entiers de K. $x_1, x_2, \ldots, x_N$ étant N indéterminées, la forme linéaire

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

s'appelle une *forme fondamentale* de K. A chaque base se trouve attachée une forme fondamentale, et l'on passe de l'une de ces formes à une autre par une substitution linéaire de déterminant ± 1 sur les indéterminées.

1° Définitions et étude préliminaire d'ensembles de décomposition et d'inertie.

Définitions 1. On appelle *ensemble de décomposition de* $\mathfrak{P}^*$ *dans* K/k et l'on désigne par $Z_{K/k}(\mathfrak{P}^*)$ l'ensemble des isomorphismes σ de K/k tels que

$$\sigma\mathfrak{P} \equiv 0 \pmod{\mathfrak{P}^*}.$$

[1] *Gött. Nachr.*, 1894, pp. 224-236; *Jahresb. d. deutsch. Math.-Ver.*, t. 4, 1894-1895, pp. 175-746.

On appelle ensemble d'inertie de $\mathfrak{P}^*$ dans K/k et l'on désigne par $T_{K/k}(\mathfrak{P}^*)$ l'ensemble des σ tels que

$$\sigma\xi \equiv \xi \pmod{\mathfrak{P}^*}.$$

Théorème 1. Si $\sigma \leqslant Z_K(\mathfrak{P}^*)$, on a non seulement $\sigma\mathfrak{P} \equiv 0 \pmod{\mathfrak{P}^*}$, mais encore

$$\sigma\mathfrak{P} \equiv 0 \pmod{\mathfrak{P}^{*a}}.$$

Démonstration. Soit

$$\mathfrak{p} = \mathfrak{P}^e \mathfrak{P}_1^{e_1} \ldots, \mathfrak{P}_s^{e_s}$$

la décomposition de $\mathfrak{p}$ en idéaux premiers de K.

Puisque $\mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2}, \ldots, \mathfrak{P}_s^{e_s}$ est premier à $\mathfrak{P}$, $\sigma(\mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2}, \ldots, \mathfrak{P}_s^{e_s})$ est premier à $\sigma\mathfrak{P}$, donc aussi à $\mathfrak{P}^*$. Il en résulte que la contribution de $\mathfrak{P}^*$ est la même dans $(\sigma\mathfrak{P})^e$ et dans $\sigma\mathfrak{p} = \mathfrak{p}$; la dernière contribution étant $\mathfrak{P}^{*ae}$, on a le théorème. C. Q. F. D.

Lemme 1. L'ordre en $\mathfrak{P}^*$ de $\sigma\xi - \xi$ est le minimum de l'ordre en $\mathfrak{P}^*$ de $\sigma\alpha - \alpha$, α parcourant les entiers de K.

Démonstration. En effet, tout entier α de K peut être obtenu en donnant aux indéterminées qui figurent dans ξ des valeurs entières rationnelles; donc l'ordre de $\sigma\alpha - \alpha$ est au moins égal à l'ordre de $\sigma\xi - \xi$. D'autre part, l'ordre de $\sigma\xi - \xi$ est le plus petit des ordres des $\sigma\alpha_i - \alpha_i$, où $\alpha_1, \alpha_2, \ldots, \alpha_N$ sont les éléments de la base qui a servi à former ξ. Donc l'ordre de $\sigma\xi - \xi$ est au moins égal au minimum de l'ordre de $\sigma\alpha - \alpha$. C. Q. F. D.

Désignons par ρ une racine primitive (mod $\mathfrak{P}$) dans K. Si $\sigma \leqslant T_K(\mathfrak{P}^*)$, on doit avoir, en vertu du lemme précédent : 1° $\sigma\mathfrak{P} \equiv 0 \pmod{\mathfrak{P}^*}$, c'est-à-dire $\sigma \leqslant Z_K(\mathfrak{P}^*)$; 2° $\sigma\rho \equiv \rho \pmod{\mathfrak{P}^*}$. Inversement, supposons ces conditions réalisées. Tout entier α de K est congru (mod $\mathfrak{P}$) à une puissance ρ^g de ρ ou à 0 : d'où, si $\alpha \not\equiv 0 \pmod{\mathfrak{P}}$, $\sigma\alpha \equiv \sigma\rho^g \pmod{\sigma\mathfrak{P}}$, donc aussi (mod $\mathfrak{P}^*$)
et

$$\sigma\alpha \equiv \sigma\rho^g \equiv \rho^g \equiv \alpha \pmod{\mathfrak{P}^*}.$$

La même congruence a évidemment lieu si $\alpha \equiv 0 \pmod{\mathfrak{P}}$. Il en résulte, en vertu du lemme 1, que $\sigma \leqslant T_K(\mathfrak{P}^*)$. Nous allons montrer mainte-

nant que la condition $\sigma < T_K(\mathfrak{P}^*)$ entraîne $\sigma\xi \equiv \xi \pmod{\mathfrak{P}^{*a}}$. Pour cela, nous avons besoin des lemmes suivants :

Lemme 2. Soient F le degré absolu de $\mathfrak{P}$ dans K et $c = p^F - 1$; soit n un entier positif quelconque. Il existe une racine primitive $\rho_n \pmod{\mathfrak{P}}$ telle que

$$\rho_n^c \equiv 1 \pmod{\mathfrak{P}^n}.$$

Démonstration. La proposition est vraie pour $n-1$. Nous la démontrerons par récurrence sur n. Supposons-la vraie pour $n-1$; π étant un nombre de K d'ordre 1 pour $\mathfrak{P}$, on a

$$\rho_{n-1}^c \equiv 1 + \alpha\pi^{n-1} \pmod{\mathfrak{P}^n},$$

où α est un entier de K. β étant un entier que nous déterminerons, posons $\rho_n = \rho_{n-1} + \beta\pi^{n-1}$; on a

$$\rho_n^c \equiv \rho_{n-1}^c + c\beta\pi^{n-1} \equiv 1 + (\alpha + c\beta)\pi^{n-1} \pmod{\mathfrak{P}^n}.$$

Il suffit donc de choisir β de telle manière que $\alpha + c\beta \equiv 0 \pmod{\mathfrak{P}}$, ce qui est toujours possible, puisque $c \not\equiv 0 \pmod{p}$.

Remarque. D'après la manière même dont nous avons construit ρ_n, on a

$$\rho_n \equiv \rho_{n-1} \pmod{\mathfrak{P}^{n-1}}.$$

Lemme 3. ρ_n étant une racine primitive $(\mathrm{mod}\ \mathfrak{P})$ dans K satisfaisant à la condition du lemme 1, on a, pour tout $\sigma < T_K(\mathfrak{P}^*)$,

$$\sigma\rho_n \equiv \rho_n \pmod{\mathfrak{P}^{*an}}.$$

Démonstration. En effet, on a

$$\sigma\rho_n^c - \rho_n^c = (\sigma\rho_n - \rho_n)(\rho_n^{c-1} + \rho_n^{c-2}\cdot\sigma\rho_n + \cdots + \sigma\rho_n^{c-1}).$$

On a $\rho_n^c \equiv 1 \pmod{\mathfrak{P}^n}$; d'où $\sigma\rho_n^c \equiv 1 \pmod{\sigma\mathfrak{P}^n}$, et, puisque $\sigma < T_K(\mathfrak{P}^*)$, donc aussi $\sigma < Z_K(\mathfrak{P}^*)$, on a $\sigma\mathfrak{P}^n \equiv 0 \pmod{\mathfrak{P}^{*an}}$. Il en résulte que

$$\sigma\rho_n^c - \rho_n^c \equiv 0 \pmod{\mathfrak{P}^{*an}}.$$

D'autre part, on a $\sigma\rho_n \equiv \rho_n \pmod{\mathfrak{P}^*}$, et par suite

$$\rho_n^{c-1} + \rho_n^{c-2}\cdot\sigma\rho_n + \cdots + \sigma\rho_n^{c-1} \equiv c\rho_n^{c-1} \not\equiv 0 \pmod{\mathfrak{P}^*},$$

ce qui démontre le lemme.

Théorème 2. Si $\sigma \leqslant T_K(\mathfrak{P}^*)$, on a non seulement $\sigma\xi \equiv \xi \pmod{\mathfrak{P}^*}$, mais encore

$$\sigma\xi \equiv \xi \pmod{\mathfrak{P}^{*a}}.$$

Démonstration. Un entier α de K est congru (mod $\mathfrak{P}$) à une puissance ρ_1^q de ρ_1 ou se divise par $\mathfrak{P}$. Dans le premier cas on a

$$\sigma\alpha \equiv \sigma\rho_1^q \equiv \rho_1^q \equiv \alpha \pmod{\mathfrak{P}^{*a}}.$$

Dans le deuxième cas on a $\sigma\alpha \equiv 0 \pmod{\sigma\mathfrak{P}}$, c'est-à-dire $\sigma\alpha \equiv 0 \equiv \alpha \pmod{\mathfrak{P}^{*a}}$; d'où le théorème.

2° Définition d'ensembles de ramification et leur étude préliminaire.

Définitions 2. σ étant un élément de $T_{K/k}(\mathfrak{P}^*)$, on appelle *nombre caractéristique de* σ *pour* $\mathfrak{P}^*$ et l'on désigne par $v(\sigma; \mathfrak{P}^*)$ le nombre $\frac{w}{a} - 1$, où w est l'ordre en $\mathfrak{P}^*$ de $\sigma\xi - \xi$.

On appelle *ensemble de ramification de* $\mathfrak{P}^*$ *dans* K/k et l'on désigne par $V_{K/k}(\mathfrak{P}^*)$ l'ensemble des éléments σ de $T_{K/k}(\mathfrak{P}^*)$ pour lesquels l'on a $v(\sigma; \mathfrak{P}^*) > 0$.

Les nombres de ramification de $\mathfrak{P}^*$ *dans* K/k sont les nombres caractéristiques d'isomorphismes $\sigma \leqslant V_{K/k}(\mathfrak{P}^*)$. Soient

$$v_0(\mathfrak{P}^*; K/k),\quad v_1(\mathfrak{P}^*; K/k), \ldots, v_{m-1}(\mathfrak{P}^*; K/k),\quad v_m(\mathfrak{P}^*; K/k) = +\infty\ (^2)$$

ces nombres supposés rangés par ordre de grandeurs croissantes; $v_q(\mathfrak{P}^*; K/k)$ s'appelle *le* q *— ième nombre de ramification* de $\mathfrak{P}^*$ dans K/k. Il est, de plus, souvent commode de poser $v_{-1}(\mathfrak{P}^*; K/k) = 0$ (3).

On appelle *niveau* d'un élément $\sigma \leqslant T_{K/k}(\mathfrak{P}^*)$, et l'on désigne par $\lambda_{K/k}(\sigma; \mathfrak{P}^*)$ l'entier $q \geqq -1$ défini par la formule

$$v(\sigma; \mathfrak{P}^*) = v_q(\mathfrak{P}^*; K/k)\ (^4).$$

---

(2) $v(\sigma; \mathfrak{P}^*)$ n'est égal à $+\infty$ que si $\sigma = 1_K$.

(3) On appellera parfois $v_{-1}(\mathfrak{P}^*; K/k)$ et $v_m(\mathfrak{P}^*; K/k)$ nombres de ramification *impropres* de $\mathfrak{P}^*$ dans K/k, et les autres $v_q(\mathfrak{P}^*; K/k)$ nombres de ramification *propres*.

(4) Cette définition ainsi que la suivante sont justifiées par le théorème 2 de ce chapitre.

On appelle *ensemble de ramification d'ordre* q $(-1 \leqq q \leqq m)$ *de* $\mathfrak{P}^*$ *dans* K/*k* et l'on désigne par $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$ l'ensemble des éléments σ de $T_{K/k}(\mathfrak{P}^*)$ pour lesquels on a

$$v(\sigma; \mathfrak{P}^*) \geqq v_q(\mathfrak{P}^*; K/k)\ (5).$$

Il résulte de ces définitions que l'on a

$$T_{K/k}(\mathfrak{P}^*) = \overset{(-1)}{V}_{K/k}(\mathfrak{P}^*); \qquad V_{K/k}(\mathfrak{P}^*) = \overset{(0)}{V}_{K/k}(\mathfrak{P}^*)$$

$$Z_{K/k}(\mathfrak{P}^*) \geqq \overset{(-1)}{V}_{K/k}(\mathfrak{P}^*) \geqq \overset{(0)}{V}_{K/k}(\mathfrak{P}^*) > \overset{(1)}{V}_{K/k}(\mathfrak{P}^*) > \cdots > \overset{(m-1)}{V}_{K/k}(\mathfrak{P}^*) > \overset{(m)}{V}_{K/k}(\mathfrak{P}^*) = \{1_K\}.$$

La suite d'ensembles écrite dans la ligne précédente s'appelle *la suite caractéristique de* $\mathfrak{P}^*$ *dans* K/*k*.

Théorème 3. σ étant un élément de $T_K(\mathfrak{P}^*)$ et π étant un entier de K d'ordre 1 en $\mathfrak{P}$, l'ordre pour $\mathfrak{P}^*$ de $\sigma\pi - \pi$ est $a[1 + v(\sigma; \mathfrak{P}^*)]$.

Démonstration. En vertu du lemme 1, l'ordre en $\mathfrak{P}^*$ de $\sigma\pi - \pi$ est au moins égal à $w = a[1 + v(\sigma; \mathfrak{P}^*)]$. Nous allons montrer qu'il ne peut être plus grand.

En effet, en vertu du lemme 1, il existe dans K un entier α tel que $\sigma\alpha - \alpha$ soit d'ordre w en $\mathfrak{P}^*$. Posons $u = 2 + E(v(\sigma; \mathfrak{P}^*))$, où $E(x)$ désigne le plus grand entier tel que $E(x) \leqq x < E(x) + 1$.

D'après le lemme 3 on peut choisir dans K une racine primitive (mod $\mathfrak{P}$) ρ telle que l'on ait, pour tout $\sigma \leqslant T_K(\mathfrak{P}^*)$,

$$\sigma\rho \equiv \rho \pmod{\mathfrak{P}^{*au}};\ \text{donc, à fortiori,}\ \pmod{\mathfrak{P}^{*w+1}}.$$

On sait que α est congru (mod $\mathfrak{P}^u$) à un nombre de la forme

$$\rho^{a_0}\pi^{n_0} + \rho^{a_1}\pi^{n_1} + \cdots + \rho^{a_s}\pi^{n_s}$$

$a_0, a_1, \ldots, a_s$ étant des entiers rationnels, $u_0, u_1, \ldots, u_s$ étant des entiers rationnels tels que $0 \leqq u_0 < u_1 < \ldots < u_s < u$. On en déduit

$$\sigma\alpha \equiv \rho^{a_0}\sigma\pi^{n_0} + \rho^{a_1}\sigma\pi^{n_1} + \cdots + \rho^{a_s}\sigma\pi^{n_s} \pmod{\mathfrak{P}^{*w+1}};$$

d'où

$$\sigma\alpha - \alpha \equiv \rho^{a_0}(\sigma\pi^{n_0} - \pi^{n_0}) + \rho^{a_1}(\sigma\pi^{n_1} - \pi^{n_1}) + \cdots + \rho^{a_s}(\sigma\pi^{n_s} - \pi^{n_s}) \pmod{\mathfrak{P}^{*w+1}}.$$

---

(5) On définissait $\overset{(q)}{V}_{K/k}$ comme l'ensemble des σ tels que $v(\sigma) \geqq v_{q+1}(K/k)$. Sur le conseil de M. Claude Chevalley, j'ai adopté la notation présente, qui est plus commode.

Or, pour tout entier $l \geqq 0$, $\sigma\pi^l - \pi^l$ est divisible par $\sigma\pi - \pi$. Donc, si w' désigne l'ordre en $\mathfrak{P}^*$ de $\sigma\pi - \pi$, le second membre est d'ordre $\geqq w'$ en $\mathfrak{P}^*$. Si l'on avait $w' > w$, on aurait $\sigma\alpha \equiv \alpha \pmod{\mathfrak{P}^{*w+1}}$, ce qui n'est pas. C. Q. F. D.

3° Influence du choix de $\mathfrak{P}^*$. — Remarquons d'abord que si K^{**} est une extension galoisienne de k contenant K^* et si $\mathfrak{P}^{**}$ est un diviseur premier de $\mathfrak{P}^*$ dans K^{**}, les ensembles de la suite caractéristique de $\mathfrak{P}^{**}$ dans K/k sont les mêmes que ceux de la suite caractéristique de $\mathfrak{P}^*$, et que l'on a, pour $\sigma \leqslant T_{K/k}(\mathfrak{P}^{**}) = T_{K/k}(\mathfrak{P}^*)$,

$$v(\sigma; \mathfrak{P}^{**}) = v(\sigma; \mathfrak{P}^*).$$

Il en résulte que la suite caractéristique de $\mathfrak{P}^*$ dans K/k et les nombres caractéristiques des $\sigma \leqslant T_{K/k}(\mathfrak{P}^*)$ pour $\mathfrak{P}^*$ ne dépendent que de l'idéal premier $\mathfrak{P}\cdot$ du corps de Galois $K\cdot$ de K qui est divisible par $\mathfrak{P}^*$.

Soit maintenant $\mathfrak{P}_1^*$ un autre diviseur premier de $\mathfrak{P}$ dans K^*. Puisque le produit des conjugués de $\mathfrak{P}^*$ par rapport à K, c'est-à-dire la norme de $\mathfrak{P}^*$ dans K^*/K, est une puissance de $\mathfrak{P}$, il existe un automorphisme σ^* de K^*/K tel que

$$\sigma^* \mathfrak{P}^* = \mathfrak{P}_1^*$$

La correspondance $\sigma \to \sigma^*\sigma$ est un automorphisme I de $G_{K/k}$. En effet, on a, si $\sigma_1, \sigma_2 \leqslant G_K$,

$$\sigma^*\sigma_1 . \sigma^*\sigma_2 = \text{corr.}_K\{\text{gen.}_{K*}(\sigma^*\sigma_1) . \text{gen.}_{K*}(\sigma^*\sigma_2)\} = \text{corr.}_K\{\sigma^* . \text{gen.}_{K*}\sigma_1 . \sigma^* . \text{gen.}_{K*}\sigma_2\}$$
$$= \text{corr.}_K\{\sigma^* . \text{gen.}_{K*}\sigma_1 . \text{gen.}_{K*}\sigma_2\} = \sigma^*(\sigma_1\sigma_2),$$

parce que, σ^* étant dans $G_{K*/K}$, on a $\text{gen.}_{K*}\sigma_1 . \sigma^* = \text{gen.}_{K*}\sigma_1$.

Il est clair que

$$I . Z_{K/k}(\mathfrak{P}^*) = Z_{K/k}(\mathfrak{P}_1^*), \qquad I T_{K/k}(\mathfrak{P}^*) = T_{K/k}(\mathfrak{P}_1^*).$$

De plus si $\sigma \leqslant T_{K/k}(\mathfrak{P}^*)$, on a

$$v(I\sigma; \mathfrak{P}_1^*) = v(\sigma; \mathfrak{P}^*)$$

et par suite I transforme la suite caractéristique de $\mathfrak{P}^*$ en la suite caractéristique de $\mathfrak{P}_1^*$. Donc a lieu

Théorème 4. Si $\mathfrak{P}_1^*$ est un autre facteur premier de $\mathfrak{P}$ dans K^*, la suite caractéristique de $\mathfrak{P}_1^*$ se déduit de celle de $\mathfrak{P}^*$ par un automorphisme de

l'hypergroupe de Galois de K/k. En particulier, le nombre d'éléments des ensembles correspondants de suites caractéristiques de $\mathfrak{P}^*$ et de $\mathfrak{P}_1^*$ est le même.

De plus, on a

$$v_q(\mathfrak{P}^*; K/k) = v_q(\mathfrak{P}_1^*; K/k) \qquad (q = -1, 0, 1, \ldots, m).$$

Il résulte de ce théorème qu'on peut remplacer dans la notation des nombres de ramification l'indication de $\mathfrak{P}^*$ par celle de $\mathfrak{P}$, et les désigner par $v_q(\mathfrak{P}; K/k)$. Aussi la notation suivante se trouve justifiée :

$z(\mathfrak{P}; K/k)$ désigne le nombre d'éléments de $Z_{K/k}(\mathfrak{P}^*)$;

$n_q(\mathfrak{P}; K/k)$ $(q = -1, 0, 1, \ldots, m)$ désigne le nombre d'éléments de $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$.

4° Ensemble Z. — Désignons par e, f resp. l'ordre et le degré de $\mathfrak{P}$ dans K/k.

Théorème 5. $z(\mathfrak{P}; K/k) = ef$.

Démonstration. Puisque $N_{K/k}(\mathfrak{P}) = \mathfrak{p}^f$, la contribution de $\mathfrak{P}^*$ dans $\prod_{\sigma \leqslant g_{K/k}} \sigma\mathfrak{P}$ $= N_{K/k}(\mathfrak{P})$ est $\mathfrak{P}^{*aef}$. D'autre part, la contribution de $\mathfrak{P}^*$ dans $\sigma\mathfrak{P}$ est $\mathfrak{P}^{*a}$ ou $\mathfrak{P}^{*0}$, suivant que σ est dans $Z_{K/k}(\mathfrak{P}^*)$ ou n'y est pas. D'où le théorème.

Théorème 6. Si $K > \overline{K} > k$,

$$Z_{\overline{K}/k}(\mathfrak{P}^*) = \mathrm{corr.}_{\overline{K}}\, Z_{K/k}(\mathfrak{P}^*).$$

Démonstration. Comme $N_{K/\overline{K}}(\mathfrak{P})$ est la puissance de l'idéal premier $\overline{\mathfrak{P}}$ de $\overline{K}$ divisible par $\mathfrak{P}^*$, $\bar{\sigma}$ est ou n'est pas dans $Z_{\overline{K}}(\mathfrak{P}^*)$, suivant que $\bar{\sigma}\, N_{K/\overline{K}}(\mathfrak{P})$ est $\equiv$ ou $\not\equiv 0 \pmod{\mathfrak{P}^*}$.

Or, d'après 3° de B du chapitre I, $\bar{\sigma} N_{K/\overline{K}}(\mathfrak{P}) = \bar{\sigma} \prod_{\sigma \leqslant G_{K/\overline{K}}} \sigma\mathfrak{P} = \prod_{\sigma \leqslant \mathrm{gen.}_K \bar{\sigma}}$ $\sigma\mathfrak{P}$ et σ est ou n'est pas dans $Z_{\overline{K}}(\mathfrak{P}^*)$, suivant que dans $\mathrm{gen.}_K\bar{\sigma}$ il y a ou il n'y a pas de σ tel que $\sigma\mathfrak{P} \equiv 0 \pmod{\mathfrak{P}^*}$, c'est-à-dire tel que $\sigma \leqslant Z_K(\mathfrak{P}^*)$. Autrement dit, $\bar{\sigma}$ est ou n'est pas dans $Z_{\overline{K}}(\mathfrak{P}^*)$, suivant qu'il est ou n'est pas dans $\mathrm{corr.}_{\overline{K}} Z_K(\mathfrak{P}^*)$. C. Q. F. D.

Conséquence 1 : $\text{corr.}_{K} Z_{K*/k}(\mathfrak{P}^*) = Z_{K/k}(\mathfrak{P}^*)$.

$Z_{K/k}(\mathfrak{P}^*)$ n'est pas, en général, un sous-hypergroupe de $G_{K/k}$ [6]. Mais le théorème précédent permet de montrer l'existence d'une loi de composition par rapport à laquelle non seulement $Z_{K/k}(\mathfrak{P}^*)$, mais aussi tous les ensembles de la suite caractéristique de $\mathfrak{P}^*$ dans K/k sont hypergroupes. Pour cela désignons par Z^* l'ensemble $Z_{K*/k}(\mathfrak{P}^*)$; Z, $\overset{(-1)}{V}$, $\overset{(0)}{V}$, ..., $\overset{(m)}{V}$ désigneront les ensembles de la suite caractéristique de $\mathfrak{P}^*$ dans K/k.

Théorème 7. $Z^{(Z^*)}$ est un hypergroupe et les $\overset{(q)}{V}$ $(q = -1, 0, 1, \ldots, m)$ sont sous-hypergroupes de $Z^{(Z^*)}$.

Démonstration. Il est évident que Z^* est un groupe; d'où, en vertu de 4° de B du chapitre I, il suit du théorème 6 de ce chapitre que Z est hypergroupe par rapport à la loi de composition induite par Z^*. Ceci posé, considérons le composé d'après la loi de composition de $Z^{(Z^*)}$ $\sigma_1 \sigma_2$ de deux éléments σ_1, σ_2 de $\overset{(q)}{V}$. Soit $\sigma \prec \sigma_1 \sigma_2$. Alors, il existent $\sigma_1^* \prec \text{gen.}_{Z^*} \sigma_1$, $\sigma_2^* \prec \text{gen.}_{Z^*} \sigma_2$ tels que $\sigma_1^* \sigma_2^* \prec \text{gen. } \sigma$. Donc

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

Or $\sigma_1 \xi - \xi \equiv 0 \pmod{\mathfrak{P}^{*a(1+v_q)}}$ et $\sigma_2 \xi - \xi \equiv 0 \pmod{\mathfrak{P}^{*a(1+v_q)}}$. Cette dernière congruence entraîne la congruence

$$\sigma_1^* (\sigma_2 \xi - \xi) \equiv 0 \pmod{\sigma_1^* \mathfrak{P}^{*a(1+v_q)} = \mathfrak{P}^{*a(1+v_q)}} \quad (\text{car } \sigma_1^* \prec Z^*);$$

d'où

$$\sigma\xi - \xi \equiv 0 \pmod{\mathfrak{P}^{*a(1+v_q)}}$$

et $\sigma \prec \overset{(q)}{V}$. Comme $Z^{(Z^*)}$ est un hypergroupe$_D$ fini, cela démontre le théorème [7].

Conséquence. $\dfrac{z(K/k; \mathfrak{P})}{n_{-1}(K/k; \mathfrak{P})}$ et tous les $\dfrac{n_q(K/k; \mathfrak{P})}{n_{q+1}(K/k; \mathfrak{P})}$ $(q = -1, 0, 1, \ldots, m-1)$ sont entiers.

En effet, $\dfrac{z}{n_{-1}}$ et les $\dfrac{n_q}{n_{q+1}}$ sont resp. les nombres d'éléments $(Z/T)^{(Z^*)}$ et de

---

[6] Voir la note 1 à la fin du travail.

[7] Cette démonstration simple et élégante de ce théorème, dont on verra l'importance dans la suite du travail, m'a été indiquée par M. Claude Chevalley, après la lecture de ma démonstration primitive, qui était beaucoup plus compliquée et beaucoup moins pure et intuitive. Je l'en remercie.

$(\overset{(q)}{\mathrm{V}} / \overset{(q+1)}{\mathrm{V}})^{(\mathrm{Z}^*)}$. Je désigne l'entier $\frac{n_q(\mathrm{K}/k;\mathfrak{P})}{n_{q+1}(\mathrm{K}/k;\mathfrak{P})}$ $(q = -1, 0, 1, \ldots, m-1)$ par $r_q(\mathrm{K}/k;\mathfrak{P})$.

5° Groupe $(\mathrm{Z}/\mathrm{T})^{(\mathrm{Z}^*)}$. — Soient r le corps des restes d'entiers de $k \pmod{\mathfrak{p}}$; $\mathfrak{R}$ celui des restes d'entiers de $\mathrm{K} \pmod{\mathfrak{P}}$; $\mathfrak{R}^*$ celui des restes d'entiers de $\mathrm{K}^* \pmod{\mathfrak{P}^*}$. On a

$$r \leqq \mathfrak{R} \leqq \mathfrak{R}^*.$$

Si ρ est une racine primitive $(\mathrm{mod}\ \mathfrak{P})$ dans K, on a $\mathfrak{R} = r(\bar{\rho})$, où $\bar{\rho}$ est la classe de restes $(\mathrm{mod}\ \mathfrak{P})$ à laquelle appartient ρ.

Soit p^{f_0} la norme absolue de $\mathfrak{p}$; r est un corps de p^{f_0} éléments et $\mathfrak{R}$ est une extension de degré f de r.

Soit σ un élément de Z. Si $\alpha + \beta \equiv \gamma$, ou $\alpha\beta \equiv \gamma$, ou $\alpha \not\equiv \beta \pmod{\mathfrak{P}^*}$, α, β, γ étant des entiers de K, ces congruences respectives ont lieu $(\mathrm{mod}\ \mathfrak{P})$; donc on a respectivement $\sigma\alpha + \sigma\beta \equiv \sigma\gamma$, $\sigma\alpha \cdot \sigma\beta \equiv \sigma\gamma$, $\sigma\alpha \not\equiv \sigma\beta \pmod{\sigma\mathfrak{P}}$, donc aussi $(\mathrm{mod}\ \mathfrak{P}^*)$: σ produit un isomorphisme de $\mathfrak{R}/r$ regardé comme un sous-corps de $\mathfrak{R}^*/r$. Comme $\mathfrak{R}/r$ est galoisien, cet isomorphisme est un automorphisme et l'on a

$$\sigma^*\bar{\rho} = \bar{\rho}^{p^{fi_0}}$$

où i est un entier rationnel; c'est-à-dire

$$\sigma\rho \equiv \rho^{p^{if_0}} \pmod{\mathfrak{P}^*}.$$

En vertu de la congruence $\rho^{p^{ff_0}} \equiv \rho \pmod{\mathfrak{P}^*}$, on peut toujours supposer $i \not\geqq f$. Comme, d'autre part, les nombres ρ, $\rho^{p^{f_0}}$, ..., $\rho^{p^{ff_0-f_0}}$ sont incongrus deux à deux $(\mathrm{mod}\ \mathfrak{P}^*)$, i est bien déterminé par cette condition. Nous désignerons par $i_k(\sigma;\mathfrak{P}^*)$ la classe de restes $(\mathrm{mod}\ f)$ à laquelle appartient i; $i(\sigma)$ est donc une fonction définie sur Z et dont les valeurs sont dans le groupe additif des restes $(\mathrm{mod}\ f)$. Nous allons étudier les propriétés de cette fonction :

a) $i(\sigma)$ *prend toutes les valeurs possibles dans le groupe additif* $(\mathrm{mod}\ f)$.

En effet, soit ρ un élément de $\bar{\rho}$ congru $0 \left(\mathrm{mod}\ \frac{\mathfrak{P}}{\mathfrak{P}^e}\right)$. Soit $\varphi(x) = 0$ l'équation

---

(8) Autres interprétations de $i_k(\sigma;\mathfrak{P}^*)$: 1° $i(\sigma)$ est l'ensemble de tous les entiers i tels que pour tout entier α de K on a $\sigma\alpha \equiv \alpha^{p^{if_0}} (\mathrm{mod}.\ \mathfrak{P}^*)$; 2° $i(\sigma)$ est l'ensemble de tous les entiers i tels que, $\xi(x_1, x_2, \ldots, x_N) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_N x_N$ étant une forme fondamentale de K, on a

$$\sigma\xi(x_1^{p^{if_0}}, x_2^{p^{if_0}}, \ldots, x_N^{p^{if_0}}) \equiv [\xi(x_1, x_2, \ldots, x_N)]^{p^{if_0}} (\mathrm{mod}\ \mathfrak{P}^*).$$

irréductible dans k auquelle satisfait ρ. Il est évident que parmi les racines de $\varphi(x) = 0$, il y en a une qui est congrue à $\rho^{p^{if_0}} \pmod{\mathfrak{P}^*}$, i étant un entier rationnel arbitraire. Soit ρ' cette racine et soit σ l'isomorphisme de K/k tel que $\sigma\rho = \rho'$. Supposons que $\sigma\mathfrak{P}$ est premier à $\mathfrak{P}^*$. Comme $\sigma\mathfrak{p} = \mathfrak{p}$ se divise par $\mathfrak{P}^*$, on a $\sigma\left(\frac{\mathfrak{p}}{\mathfrak{P}^e}\right) \equiv 0 \pmod{\mathfrak{P}^*}$. Il en résulte que $\sigma\rho \equiv 0 \left[\mathrm{mod}\ \sigma\left(\frac{\mathfrak{p}}{\mathfrak{P}^e}\right)\right]$ est divisible par $\mathfrak{P}^*$, c'est-à-dire $\rho' \equiv \rho^{p^{if_0}} \equiv 0 \pmod{\mathfrak{P}^*}$, ce qui est absurde. Donc $\sigma \leqslant Z_K(\mathfrak{P}^*)$ et $i(\sigma) \geqslant i$; i étant arbitraire, la proposition est exacte [1].

b) *La condition nécessaire et suffisante pour que* $i(\sigma) \equiv 0$ *est que* $\sigma \leqslant T$. C'est évident.

c) *si* $\sigma_1, \sigma_2 \leqslant Z$ *et la loi de composition est celle induite par* Z^*,

$$i_k(\sigma_1\sigma_2; \mathfrak{P}^*) = i_k(\sigma_1; \mathfrak{P}^*) + i_k(\sigma_2; \mathfrak{P}^*).$$

En effet, soient $i_1 \leqslant i(\sigma_1)$ et $i_2 \leqslant i(\sigma_2)$. On a

$$\sigma_1\sigma_2\rho = \{\sigma^*\sigma_2\rho\}_{\sigma^* \leqslant \mathrm{gen}.K^*\sigma_1} \equiv \{\sigma^*\rho^{p^{i_2 f_0}}\}_{\sigma^* \leqslant \mathrm{gen}.Z^*\sigma_1} \pmod{\sigma^*\mathfrak{P}^*}.$$

Or, $\sigma^*\mathfrak{P}^* = \mathfrak{P}^*$ et $\sigma^*\rho \equiv \rho^{p^{i_1 f_0}}$; d'où $\sigma_1\sigma_2\rho \equiv \rho^{p^{(i_1+i_2)f_0}} \pmod{\mathfrak{P}^*}$.

C. Q. F. D.

Théorème 8. $T^{(Z^*)}$ est un sous-hypergroupe invariant de $Z^{(Z^*)}$, $(Z/T)^{(Z^*)}$ est un groupe cyclique d'ordre f dont l'isomorphie avec le groupe additif des entiers (mod f) se réalise par la correspondance $\sigma \to i_k(\sigma; \mathfrak{P}^*)$.

Démonstration. — Si $\sigma_1 \leqslant \sigma T$, on a $i(\sigma_1) = i(\sigma) + 0 = i(\sigma)$. Si $i(\sigma_1) = i(\sigma)$, choisissons σ_2 tel que $\sigma_1 \leqslant \sigma\sigma_2$ (cela est possible d'après la définition de l'hypergroupe). On a $i(\sigma_2) = (i\sigma_1) - i(\sigma) = 0$, donc $\sigma_2 \leqslant T$ et $\sigma_1 \leqslant \sigma T$. Il s'ensuit, d'après *a*) et *c*), tout, sauf l'invariance de T dans Z.

Pour la démontrer, considérons $T\sigma$; on a $i(T\sigma) = i(T) + i(\sigma) = i(\sigma)$; d'où $T\sigma \leqq \sigma T$. Mais la loi de composition des $i(\sigma)$ étant commutative, on a aussi $\sigma T \leqq T\sigma$. D'où $T\sigma = \sigma T$. C. Q. F. D.

---

[9] En particulier, si $e = 1$, c'est-à-dire $T = \{1_K\}$, la condition $i(\sigma) = 1$ détermine un $\sigma \leqslant Z$ qui sera désigné par $\left(\frac{K/k}{\mathfrak{P}^*}\right)$ et qui généralise le symbole de Frobenius.

[10] A et B étant deux ensembles de nombres, j'écris $A \equiv B$ (mod. $\mathfrak{L}$) quand on peut établir une correspondante biunivoque entre A et B de manière que chaque $a \leqslant A$ soit congru (mod. $\mathfrak{L}$) à son correspondant $b \leqslant B$.

Congruence $a \equiv \{b\}$ (mod. $\mathfrak{L}$) doit être regardée comme équivalente à $a \equiv b$ (mod. $\mathfrak{L}$).

Théorème 9. $\frac{z(K/k;\mathfrak{P})}{n_{-1}(K/k;\mathfrak{P})} = f$; $n_{-1}(K/k;\mathfrak{P}) = e$.

Démonstration. — $\frac{z}{n_{-1}}$ est l'ordre de $(Z/T)^{(Z^*)}$ qui est bien f. Comme $z = ef$, on a

$$n_{-1} = \frac{z}{f} = e. \qquad \text{C. Q. F. D.}$$

6° Un théorème auxiliaire. — Posons

$$T^* = T_{K/k}(\mathfrak{P}^*); \qquad V^* = V_{K/k}(\mathfrak{P}^*).$$

Nous voulons démontrer que $T = \text{corr}_K T^*$ et $V = \text{corr}_K V^*$. Pour cela on va se servir du théorème n° 40 de Hilbert, dont on trouve la démonstration dans sa *Théorie des corps de nombres algébriques*, p. 39.

Soit φ une forme dans un corps algébrique. Le *contenu* de φ (c'est-à-dire le p. g. c. d. de ses coefficients) sera désigné par $\overline{\varphi}$. Le théorème de Hilbert se formule ainsi :

Théorème. Soient K, K' deux extensions finies de k tels que $K' > K$. Soient ξ, ξ' des formes fondamentales de ces corps. Si $\sigma \leqslant G_{K/k}$, on a

$$\overline{\sigma\xi - \xi} = \prod_{\sigma' \leqslant \text{gen}_{K'}\sigma} (\overline{\sigma'\xi' - \xi'}).$$

Nous basant sur ce théorème de Hilbert nous allons démontrer le théorème suivant :

Théorème 10. Si $K' > K$, $T_K(\mathfrak{P}^*) = \text{corr}_K T_{K'}(\mathfrak{P}^*)$ et $V_K(\mathfrak{P}^*) = \text{corr.}_K V_{K'}(\mathfrak{P}^*)$.

Démonstration. $\sigma\xi - \xi \equiv$ ou $\not\equiv 0 \pmod{\mathfrak{P}^*}$ suivant qu'il existe ou n'existe pas un $\sigma' \leqslant \text{gen}_{K'}\sigma$ tel que $\sigma'\xi' - \xi' \equiv 0 \pmod{\mathfrak{P}^*}$, d'où la première partie du théorème. Supposons $\sigma \leqslant T_K$.

Alors $\text{gen}_{K'}\sigma \wedge T_{K'}$ n'est pas vide, et comme $T_{K'}^{(Z^*)}$ est un hypergroupe, $\text{gen}_{K'}\sigma \wedge T_{K'}$ a, en vertu de 4° de B du chapitre I, le nombre d'éléments égal à celui de $G_{K'/K} \wedge T_{K'} = T_{K'/K}$, c'est-à-dire égal à l'ordre de l'idéal premier $\mathfrak{P}'$ dans K'/K. Si e, e' désignent les ordres de $\mathfrak{P}$ et de $\mathfrak{P}'$ par rapport à k, ce nombre d'éléments est donc $\frac{e'}{e}$. Soient $\mathfrak{P}^{*a}$, $\mathfrak{P}^{*a'}$ les contributions de $\mathfrak{P}^*$ dans $\mathfrak{P}$ et dans $\mathfrak{P}'$. Si $\text{gen}_{K'}\sigma \wedge V_{K'}$ est vide, la contribution de $\mathfrak{P}^*$ dans $\sigma\xi - \xi$ est

$(\mathfrak{P}^{*a'})^{\frac{e'}{e}} = \mathfrak{P}^{*a}$ et σ n'est pas dans V_K. Si $\text{gen}_{K'}\, \sigma \wedge V_{K'}$ n'est pas vide, l'ordre de $\sigma\xi - \xi$ en $\mathfrak{P}^*$ dépasse $a' \frac{e'}{e} = a$ et $\sigma \leqslant V_K$. C. Q. F. D.

Ce théorème entraîne $T = \text{corr.}_K T^*$ et $V = \text{corr.}_K V^*$ si l'on pose $K' = K^*$.

7° Fonction $\beta_{-1}(\sigma)$. Groupe $(T/V)^{(T^*)}$ et hypergroupe $(T/V)^{(Z^*)}$. — Soit π un nombre de K d'ordre 1 pour $\mathfrak{P}$. Faisons correspondre à chaque $\sigma \leqslant T$ la classe de restes de K^* (mod $\mathfrak{P}^*$) qui contient $\frac{\sigma\pi}{\pi}$ (on remarquera que $\frac{\sigma\pi}{\pi}$ est entier pour $\mathfrak{P}^*$, puisque $\sigma \leqslant Z$). Nous définissons ainsi une fonction $\beta_{-1}(\sigma; \mathfrak{P}^*)$ dont les valeurs sont dans $\mathfrak{R}^*$, et dont nous allons étudier les propriétés :

a) *La valeur de* $\beta_{-1}(\sigma)$ *ne dépend pas du nombre* π *qui a été choisi pour la définir.*

En effet, soit π' un autre nombre de K d'ordre 1 pour $\mathfrak{P}$. On a $\pi' \equiv \alpha\pi \pmod{\mathfrak{P}^2}$, où α est un entier de K premier à $\mathfrak{P}$. D'où, si $\sigma \leqslant T$,

$$\sigma\pi' \equiv \sigma\alpha \cdot \pi \cdot \frac{\sigma\pi}{\pi} \equiv \frac{\sigma\alpha}{\alpha}\frac{\sigma\pi}{\pi}\pi' \pmod{\sigma\mathfrak{P}^2}.$$

Or, on a $\frac{\sigma\alpha}{\alpha} \equiv 1 \pmod{\mathfrak{P}^*}$ et $\mathfrak{P}^* \mid \sigma\mathfrak{P}$; d'où

$$\frac{\sigma\pi'}{\pi'} \equiv \frac{\sigma\pi}{\pi} \pmod{\mathfrak{P}^*}.$$

b) *La condition nécessaire et suffisante pour que* $\sigma \leqslant V$ *est que* $\beta_{-1}(\sigma) = 1$.

En effet, la condition $\frac{\sigma\pi}{\pi} \equiv 1 \pmod{\mathfrak{P}^*}$ équivaut à la condition $\sigma\pi - \pi \equiv 0 \pmod{\mathfrak{P}^{*a+1}}$, donc à la condition $v(\sigma; \mathfrak{P}^*) > 0$.

Considérons deux éléments σ_1, σ_2 de T et soient $\sigma_1^* \leqslant \text{gen.}_{Z^*}\sigma_1$, $\sigma_2^* \leqslant \text{gen.}_{Z^*}\sigma_2$. Soit $\sigma = \text{corr.}_K(\sigma_1^*\sigma_2^*)$. On a

$$\frac{\sigma\pi}{\pi} = \frac{\sigma_1^*\sigma_2^*\pi}{\pi} = \sigma_1^*\left(\frac{\sigma_2^*\pi}{\pi}\right)\cdot\frac{\sigma_1^*\pi}{\pi} = \sigma_1^*\left(\frac{\sigma_2\pi}{\pi}\right)\frac{\sigma_1\pi}{\pi}.$$

F étant le degré absolu de $\mathfrak{P}$ dans K, désignons par $\mathfrak{z}$ l'automorphisme $\bar{\alpha}^* \to \bar{\alpha}^{*p^F}$ de $\mathfrak{R}^*/\mathfrak{R}$ (où $\bar{\alpha}^*$ est élément arbitraire de $\mathfrak{R}^*$).

D'après théorème 10, $\text{gen.}_{Z^*}\sigma_1 = \sigma_1^*(G_{K^*/K} \wedge Z^*) = \sigma_1^* Z_{K^*/K}$ contient un élément $\sigma_{1,0}^*$ de T^*. Donc

$$\sigma_1^* = \sigma_{1,0}^*\sigma_z^* \qquad \text{ou} \qquad \sigma_z^* \leqslant Z_{K^*/K}.$$

Il en résulte, en vertu de la propriété *c*) de $i(\sigma)$, que $i_k(\sigma_1^*) = i_k(\sigma_z^*) = f \cdot i_K(\sigma_z^*)$. Donc si $i \leqslant i_K(\sigma_z^*)$, on a

$$\sigma_1^* \left(\frac{\sigma_2 \pi}{\pi}\right) \equiv \left(\frac{\sigma_2 \pi}{\pi}\right)^{p^{iF}} \pmod{\mathfrak{P}^*};$$

d'où il résulte que

$$\beta_{-1}(\sigma) = \beta_{-1}(\sigma_1) \cdot \mathfrak{Z}^i \beta_{-1}(\sigma_2).$$

De ce résultat on déduit successivement :

c_1) *La loi de composition étant celle de* $T^{(T^*)}$, *on a, si* $\sigma_1, \sigma_2 \leqslant T$,

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

En effet $\sigma_1 \sigma_2$ est l'ensemble de tous les $\text{corr.}_K(\sigma_1^* \sigma_2^*)$, où $\sigma_1^* \leqslant \text{gen.}_{T^*} \sigma$, c'est-à-dire $i_K(\sigma_z^*) = 0$.

$\bar{\alpha}^*$ étant un élément de $\mathfrak{R}^*$, désignons par $<\bar{\alpha}^*>_F$ l'ensemble de tous les $\mathfrak{Z}^i \bar{\alpha}^*$ distincts; on a :

c_2) *La loi de composition étant celle de* $T^{(Z^*)}$, *on a, si* $\sigma_1, \sigma_2 \leqslant T$,

$$\beta_{-1}(\sigma_1 \sigma_2) = \beta_{-1}(\sigma_1) \cdot < \beta_{-1}(\sigma_2) >_F.$$

En effet, à présent σ_1^* parcourt $\text{gen.}_{Z^*} \sigma_1 = \sigma_{1,0}^* Z_{K^*/K}$ et σ_z^* parcourt $Z_{K^*/K}$. Donc $i_K(\sigma_z^*)$ parcourt le groupe additif entier des restes (mod f_K^*), où f_K^* est le degré de $\mathfrak{P}^*$ dans K^*/K, et i peut prendre toute valeur. C. Q. F. D.

Ceci posé, la propriété c_1) donne :

Théorème 11. $V^{(T^*)}$ est un sous-hypergroupe invariant de $T^{(T^*)}$; $(V/T)^{(T^*)}$ est un groupe et la correspondance $\sigma \to \beta_{-1}(\sigma)$ établit un isomorphisme entre ce groupe et un sous-groupe $M_{-1}(K/k; \mathfrak{P}^*)$ (ce groupe, à isomorphie près, ne dépend pas du choix de $\mathfrak{P}^* \mid \mathfrak{P}$) du groupe multiplicatif de classes ($\neq 0$) de restes (mod $\mathfrak{P}^*$) dans K^*.

Démonstration. Analogue à celle du théorème 8. Il faut seulement remplacer l'addition par la multiplication et 0 par 1.

Conséquence 1. On sait que le groupe multiplicatif de classes ($\neq 0$) de restes (mod $\mathfrak{P}^*$) dans K^* est cyclique d'ordre premier à p. Donc le groupe $(V/T)^{(T^*)}$ est cyclique et son ordre, égal à $r_{-1}(K/k; \mathfrak{P})$, est premier à p.

De plus, K^0/k désignant le corps de Galois de K/k, $\mathfrak{P}^0$ un idéal premier de K^0 divisant $\mathfrak{P}$, F^0 le degré absolu de $\mathfrak{P}^0$ dans K^0, on peut poser $K^* = K^0$. Le groupe multiplicatif de classes ($\neq 0$) de restes (mod $\mathfrak{P}^0$) dans K^0 est d'ordre $p^{F^0} - 1$. On a donc

Conséquence. $p^{F^0} - 1 \equiv 0 \ [\mathrm{mod}\ r_{-1}(K/k; \mathfrak{P})]$.

La propriété c_2) de $\beta_{-1}(\sigma)$ donne

Théorème 12. $V^{(Z^*)}$ est sous-hypergroupe semi-invariant de $T^{(Z^*)}$; $\sigma \to \beta_{-1}(\sigma)$ établit un isomorphisme de $(T/V)^{(Z^*)}$ à $M_{-1}(K/k; \mathfrak{P}^*)$ organisé en hypergroupe par la loi de composition

$$a * b = a \cdot < b >_F.$$

Démonstration. La deuxième partie de ce théorème est évidente d'après le théorème 10 et c_2). Quant à la première, soient $(\sigma V)^{(Z^*)}$, $(V\sigma)^{(\cdot^*)}$ les composés d'après la loi de composition de $T^{(Z^*)}$ de V par σ et de σ par V, et soient $(\sigma V)^{(T^*)}$ et $(V\sigma)^{(T^*)}$ ceux d'après la loi de composition de $T^{(T^*)}$ (on suppose $\sigma \leqslant T$). D'après une remarque de 4° de B du chapitre I on a

$$(V\sigma)^{(Z^*)} \geqq (V\sigma)^{(T^*)}; \qquad (\sigma V)^{(Z^*)} \geqq (\sigma V)^{(T^*)}.$$

Or $(\sigma V)^{(Z^*)}$ et $(\sigma V)^{(T^*)}$ étant les classes suivant V dans un hypergroupe$_D$, ces deux ensembles ont le nombre d'éléments égal à celui de V. D'où $(\sigma V)^{(Z^*)} = (\sigma V)^{(T^*)}$. Comme $(\sigma V)^{(T^*)} = (V\sigma)^{(T^*)}$, on a

$$(V\sigma)^{(Z^*)} \geqq (V\sigma)^{(T^*)} = (\sigma V)^{(T^*)} = (\sigma V)^{(Z^*)}. \qquad \text{C. Q. F. D.}$$

Conséquence. Si $\beta_{-1}(A)$ est un groupe multiplicatif, on a, la loi de composition étant celle de $T^{(Z^*)}$ et σ étant dans T,

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

Démonstration. En effet, si

$$\bar{\alpha}^* \leqslant \beta_{-1}(A), \quad \text{on a} \quad \mathfrak{Z}^i \bar{\alpha}^* = \bar{\alpha}^{*p^{iF}} \leqslant \beta_{-1}(A);$$

d'où

$$< \beta_{-1}(A) >_F = \beta_{-1}(A) \quad \text{et} \quad \beta_{-1}(\sigma A) = \beta_{-1}(\sigma) \cdot < \beta_{-1}(A) >_F = \beta_{-1}(\sigma)\beta_{-1}(A). \qquad \text{C. Q. F. D.}$$

Théorème 13. La condition nécessaire et suffisante pour que $(A/V)^{(Z^*)}$ soit un sous-hypergroupe de $(T/V)^{(Z^*)}$ est que $\beta_{-1}(A)$ soit un groupe multiplicatif.

Démonstration. On a $< \beta_{-1}(A) >_F \geqq \beta_{-1}(A)$. Si $\beta_{-1}(A)$ est groupe multiplicatif et $(A/V)^{(Z^*)}$ a un sens, on a $< \beta_{-1}(A) >_F = \beta_{-1}(A)$ et $\beta_{-1}(AA) = \beta_1(A) . \beta_{-1}(A) = \beta_{-1}(A)$; d'où $AA = AAV = AV = A$. Inversement, soit $AA = A$. Alors

$$\beta_{-1}(A)\,\beta_{-1}(A) \leqq \beta_{-1}(A) . < \beta_{-1}(A) >_F = \beta_{-1}(AA) = \beta_{-1}(A).$$

Comme $A \geqslant 1_K$ quand $AA = A$, $\beta_{-1}(A) \geqslant 1$ et $\beta_{-1}(A) \cdot \beta_{-1}(A) \geqq \beta_{-1}(A)$. Il en résulte que $\beta_{-1}(A)$ est un groupe multiplicatif. Le théorème est démontré.

8° L'ÉTUDE DES $\overset{(q)}{V}$ $(q = 0, 1, \ldots, m)$. — Soient $q \geqq 0$ et $\sigma \prec \overset{(q)}{V}$. π ayant la même signification que dans 7°, choisissons dans K^* un nombre π' dont l'ordre u pour $\mathfrak{P}^*$ est diviseur de $av_q(K/k ; \mathfrak{P})$. En particulier, si cet ordre est égal à 1, π' sera noté π^*.

Désignons par $\beta_q(\sigma ; \pi', \mathfrak{P}^*)$ la classe de restes (mod $\mathfrak{P}^*$) dans K^* à laquelle appartient $\dfrac{\sigma\pi - \pi}{\pi\pi'^{\frac{av_q}{u}}}$. On constate facilement que cette classe ne dépend pas du choix de π, qu'en changeant π' on fait subir aux $\beta_q(\sigma ; \pi', \mathfrak{P}^*)$ de tous les $\sigma \geqslant \overset{(q)}{V}$ la multiplication par un même facteur non nul. Je me borne à étudier le symbole $\beta_q(\sigma ; \pi^*, \mathfrak{P}^*)$ (c'est-à-dire, je me borne au cas $u = 1$) et à déduire de cette étude la seule propriété du symbole plus général $\beta_q(\sigma ; \pi', \mathfrak{P}^*)$ qui sera nécessaire pour une démonstration du chapitre IV. $\beta_q(\sigma ; \pi^*, \mathfrak{P}^*)$ est une fonction définie dans $\overset{(q)}{V}$ et à valeurs dans $\mathfrak{R}^*$. Elle jouit des propriétés suivantes :

a) *La condition nécessaire et suffisante pour que* $\sigma \prec \overset{(q+1)}{V}$ *est que* $\beta_q(\sigma) = 0$ · c'est évident.

Soient σ_1, σ_2 deux éléments de $\overset{(q)}{V}$; soient $\sigma_1^* \prec \text{gen.}_{Z^*}\sigma_1$, $\sigma_2^* \prec \text{gen.}_{Z^*}\sigma_2$ et $\sigma = \text{corr.}_K(\sigma_1^*\,\sigma_2^*)$. On a

$$\frac{\sigma\pi - \pi}{\pi\pi^{*av_q}} = \frac{\sigma_1^*\sigma_2^*\pi - \pi}{\pi\pi^{*av_q}} = \sigma_1^*\left(\frac{\sigma_2^*\pi - \pi}{\pi\pi^{*av_q}}\right)\cdot\frac{\sigma_1^*\pi}{\pi}\cdot\left(\frac{\sigma^*\pi^*}{\pi^*}\right)^{av_q} + \frac{\sigma_1^*\pi - \pi}{\pi\pi^{*av_q}} \equiv$$

$$\equiv \sigma_1^*\left(\frac{\sigma_2^*\pi - \pi}{\pi\pi^{*av_q}}\right)\cdot\frac{\sigma_1\pi}{\pi}\cdot\left(\frac{\sigma_1^*\pi^*}{\pi^*}\right)^{av_q} + \frac{\sigma_1\pi - \pi}{\pi\pi^{*av_q}} \qquad (\text{mod } \mathfrak{P}^*).$$

D'après ce qui a été dit dans 7° de ce chapitre il existe des i tels que

$$\sigma_1^*\left(\frac{\sigma_2\pi-\pi}{\pi\pi^{*av_q}}\right)\equiv\left(\frac{\sigma_2\pi-\pi}{\pi\pi^{*av_q}}\right)^{p^iF}\pmod{\mathfrak{P}^*}$$

et quand σ_1^* parcourt $\mathrm{gen.}_{Z^*}\sigma$, i parcourt l'ensemble de tous les entiers.

Comme $\sigma_1 \leqslant V$, on a $\frac{\sigma_1\pi}{\pi}\equiv 1 \pmod{\mathfrak{P}^*}$. Donc, si $\lambda(\sigma_1^*)$ est la classe de restes (mod $\mathfrak{P}^*$) dans K^* à laquelle appartient $\left(\frac{\sigma_1^*\pi^*}{\pi^*}\right)^{av_q}$, on a

$$\beta_q(\sigma)=\beta_q(\sigma_1)+\lambda(\sigma_1^*).\mathfrak{Z}^i\beta_q(\sigma_2).$$

Nous allons nous occuper de la question : Quel ensemble parcourt $\lambda(\sigma_1^*)$ quand σ_1^* parcourt l'ensemble de tous les $\sigma_1^* \leqslant \mathrm{gen.}_{Z^*}\sigma_1$ pour lesquels i a une valeur donnée?

Pour résoudre cette question il faut d'abord étudier la structure des $\overset{(q)}{V}$ en se servant des hypergroupes $(\overset{(q)}{V}/\overset{(q+1)}{V})^{(V^*)}$. Envisageons $\overset{(q)}{V}^{(V^*)}$. On a

b_1) *Si* σ_1, $\sigma_2 \leqslant V$ *et la loi de composition est celle de* $\overset{(q)}{V}^{(V^*)}$, *on a*

$$\beta_q(\sigma_1\sigma_2;\pi^*,\mathfrak{P}^*)=\beta_q(\sigma_1;\pi^*,\mathfrak{P}^*)+\beta_q(\sigma_2;\pi^*,\mathfrak{P}^*).$$

En effet, si $\sigma \leqslant \sigma_1\sigma_2$, on a, dans l'hypothèse de l'énoncé, $\sigma_1^* \leqslant V^*$; d'où $\mathfrak{Z}^i=\mathfrak{Z}^0$ et $\lambda(\sigma_1^*)=1$.

On déduit de là

Théorème 14. $\overset{(q)}{V}^{(V^*)}$ est un sous-hypergroupe invariant de $\overset{(q)}{V}^{(V^*)}$ et la fonction $\beta_q(\sigma;\pi^*,\mathfrak{P}^*)$ établit un isomorphisme entre $(\overset{(q)}{V}/\overset{(q+1)}{V})^{(V^*)}$ et un sous-groupe $M_q(K/k;\pi^*,\mathfrak{P}^*)$ du groupe additif des classes d'entiers de K^* (mod $\mathfrak{P}^*$).

Démonstration. Analogue à celle du théorème 8.

Conséquence. $M_q(K/k;\pi',\mathfrak{P}^*)=\beta_q(V;\pi',\mathfrak{P}^*)$ est un module et la correspondance $\sigma \to \beta_q(\sigma;\pi',\mathfrak{P}^*)$ est un isomorphisme de $(\overset{(q)}{V}/\overset{(q+1)}{V})^{(V^*)}$ à ce module

$M_q(K/k;\pi^*,\mathfrak{P})$ est un groupe additif de type $(p, p, \ldots, p)$. Il en résulte

Théorème 15. Si $q \geq 0$ on a : 1°) $(\overset{(q)}{V}/\overset{(q+1)}{V})^{(V^*)}$ est un groupe abelien de type $(p, p, \ldots, p)$ et du rang $\leq F^0$.

2°) $r_q(\mathrm{K}/k;\mathfrak{P})$ et $n_q(\mathrm{K}/k;\mathfrak{P})$ sont puissances de p.

Je désigne

$$r_q(\mathrm{K}/k;\mathfrak{P}) = p^{l_q(\mathrm{K}/k;\mathfrak{P})}; \qquad n_q(\mathrm{K}/k;\mathfrak{P}) = p^{j_q(\mathrm{K}/k;\mathfrak{P})} \qquad (q \geqq 0).$$

On a $$l_q(\mathrm{K}/k;\mathfrak{P}) \leqq \mathrm{F}^0.$$

On tire du théorème 15 la

Conséquence. $n_0(\mathrm{K}/k;\mathfrak{P})$ est une puissance de p. $r_{-1}(\mathrm{K}/k;\mathfrak{P})$ est le plus grand facteur de e premier à p. $n_0(\mathrm{K}/k;\mathfrak{P})$ est la contribution de p dans e.

Maintenant nous sommes en état de résoudre le problème posé précédemment. On a

$$\pi \equiv \alpha\pi^{*a} = \alpha\pi^{*r_{-1}(\mathrm{K}^*/\mathrm{K};\mathfrak{P}^*)\, n_0(\mathrm{K}^*/\mathrm{K};\mathfrak{P}^*)}, \qquad \text{où} \qquad \alpha \not\equiv 0 \pmod{\mathfrak{P}^*}.$$

Donc

$$1 \equiv \frac{\sigma_1\pi}{\pi} \equiv \frac{\sigma_1^*\alpha}{\alpha} \cdot \left(\frac{\sigma_1^*\pi^*}{\pi^*}\right)^{r_{-1}(\mathrm{K}^*/\mathrm{K};\mathfrak{P}^*)\cdot p^{j_0}(\mathrm{K}^*/\mathrm{K};\mathfrak{P}^*)} \pmod{\mathfrak{P}^*}.$$

On a $\dfrac{\sigma_1^*\alpha}{\alpha} \equiv \alpha^{p^{i\mathrm{F}}-1}$. Posons $\alpha = \alpha^{*a}$. On trouve que

$$\frac{\sigma_1^*\pi^*}{\pi^*} \equiv \alpha^{*1-p^{i\mathrm{F}}}\zeta \pmod{\mathfrak{P}^*}$$

où

$$\zeta^{r_{-1}} \equiv 1 \pmod{\mathfrak{P}^*}.$$

On a

$$\mathrm{gen}._{\mathrm{Z}^*}\sigma_1 = \sigma_1^* \cdot \mathrm{Z}_{\mathrm{K}^*/\mathrm{K}}.$$

Il en résulte que l'ensemble de $\sigma^* \leqslant \mathrm{gen}._{\mathrm{Z}^*}\sigma_1$ ayant le même i que σ_1^* est

$$\sigma_1^*\mathrm{T}_{\mathrm{K}^*/\mathrm{K}}.$$

Or, si $\sigma^* \leqslant \mathrm{T}_{\mathrm{K}^*/\mathrm{K}}$, on a

$$\frac{\sigma_1^*\sigma^*\pi^*}{\pi^*} = \sigma_1^*\left(\frac{\sigma^*\pi}{\pi}\right) \cdot \frac{\sigma_1^*\pi}{\pi} \equiv \left(\frac{\sigma^*\pi}{\pi}\right)^{p^{i\mathrm{F}}} \cdot \alpha^{*1-p^{i\mathrm{F}}}\zeta.$$

Mais, le reste de $\dfrac{\sigma^*\pi}{\pi}$ parcourt le groupe de racines $r_{-1}(\mathrm{K}^*/\mathrm{K};\mathfrak{P}^*)$ — ièmes de l'unité (mod $\mathfrak{P}^*$) quand σ^* parcourt $\mathrm{T}_{\mathrm{K}^*/\mathrm{K}}$. Donc le reste (mod $\mathfrak{P}^*$) de $\left(\dfrac{\sigma^*\pi}{\pi}\right)^{p^{i\mathrm{F}}}\zeta$ parcourt aussi le même groupe.

Il en résulte, δ_q étant le plus grand facteur premier à p du dénominateur de v_q, que $\overline{\alpha^*}^{-av_q(1-p^{i\mathrm{F}})}\,\lambda(\sigma_1^*)$ [11] parcourt le groupe de racines δ_q — ièmes de

---

[11] $\overline{\alpha^*}$ désigne la classe (mod $\mathfrak{P}^*$) à laquelle appartient α^*.

l'unité quand σ_1^* parcourt tous les $\sigma_1^* \leqslant \text{gen.}_{K^*}\sigma_1$ avec un i donné. Désignons le groupe des racines $\bar{\delta}_q$ — ièmes de l'unité dans $\mathfrak{R}^*$ par $\mathfrak{E}_{\bar{\delta}_q}$ et posons, si $\bar{\alpha}^* \leqslant \mathfrak{R}^*$,

$$[\bar{\alpha}^*]_{\delta_q} = \bar{\alpha}^* \cdot \mathfrak{E}_{\delta_q}.$$

On a immédiatement les deux théorèmes suivants :

b_2) *Si* $\sigma_1\sigma_2 \leqslant \overset{(q)}{V}$ *et si la loi de composition est celle de* $\overset{(q)}{V}{}^{(T^*)}$, on a

$$\beta_q(\sigma_1\sigma_2) = \beta_{-1}(\sigma_1) + [\beta_{-1}(\sigma_2)]_{\bar{\delta}_q}.$$

En effet, si $\sigma \leqslant \sigma_1\sigma_2$, on a, sous l'hypothèse de l'énoncé, que $\sigma_1^* \leqslant T_{K^*/K}$, d'où $\mathfrak{Z}^i = \mathfrak{Z}^0$, $\alpha^{*-av_q(1-q^{iF})} = 1 \pmod{\mathfrak{P}^*}$; donc l'ensemble de tous les $\lambda(\sigma_1^*)$, $\sigma_1^* \leqslant \text{gen.}_{T^*}\sigma_1$, est $\mathfrak{E}_{\bar{\delta}_q}$ et

$$\beta_q(\sigma_1\sigma_2) = \beta_q(\sigma_1) + \mathfrak{E}_{\bar{\delta}_q}\beta_q(\sigma_2) = \beta_q(\sigma_1) + [\beta_q(\sigma_2)]_{\bar{\delta}_q}. \qquad \text{C. Q. F. D.}$$

On en tire

Théorème 16. $\overset{(q+1)}{V}{}^{(T^*)}$ est un sous-hypergroupe semi-invariant de $\overset{(q)}{V}{}^{(T^*)}$ et $\sigma \to \beta_q(\sigma)$ établit un isomorphisme de $(\overset{(q)}{V} / \overset{(q+1)}{V})^{(T^*)}$ avec l'ensemble $\mathbf{M}_q(K/k)$ organisé par la loi de composition donnée par

$$a * b = a + [b]_{\bar{\delta}_q}.$$

Démonstration. Analogue à celle du théorème 11.

On voit d'après ce théorème que $\mathbf{M}_q(K/k)$ admet comme opérateur la multiplication par toute racine $\bar{\delta}_q$ — ième de l'unité dans $\mathfrak{R}^*$. Donc, c'est un module par rapport au corps fini que ces racines engendrent dans $\mathfrak{R}^*$. Il en résulte facilement que $r_q(K/k; \mathfrak{P}) \equiv 1 \pmod{\bar{\delta}_q}$.

b_3) *Si* $\sigma_1\sigma_2 \leqslant \overset{(q)}{V}$, *et si la loi de composition est celle de* $\overset{(q)}{V}{}^{(Z^*)}$, *on a*

$$\bar{\alpha}^{*-av_q}\beta_q(\sigma_1\sigma_2; \pi^*, \mathfrak{P}^*) = \bar{\alpha}^{*-av_q}\beta_q(\sigma_1; \pi^*, \mathfrak{P}^*) + [< \bar{\alpha}^{*-av_q}\beta_q(\sigma_2; \pi^*, \mathfrak{P}^*) >_F]_{\bar{\delta}_q}.$$

En effet, on a

$$\bar{\alpha}^{*-av_q}\beta_q(\sigma) = \bar{\alpha}^{*-av_q}\beta_q(\sigma_1) + \mathfrak{Z}^i\beta_q(\sigma_2)\cdot\bar{\alpha}^{*-av_q}\cdot\lambda(\sigma_1^*) = \bar{\alpha}^{*-av_q}\beta_q(\sigma_1) +$$
$$+ \mathfrak{Z}^i(\bar{\alpha}^{*-av_q}\beta_q(\sigma_2))\cdot\bar{\alpha}^{*-av_q(1-p^{iF})}\lambda(\sigma_1^*).$$

Quand σ parcourt $\sigma_1\sigma_2$, d'après ce qui précède l'expression du côté droit de cette égalité parcourt

$$\bar{\alpha}^{*-av_q}\beta_q(\sigma_1)+\{\mathfrak{Z}^i(\bar{\alpha}^{*-av_q}\beta_q(\sigma_2))\}_{(i=0,1,\ldots,n,\ldots)}\mathfrak{E}_{\bar{\delta}_q}=\bar{\alpha}^{*-av_q}\beta_q(\sigma_1)+$$
$$+[<\bar{\alpha}^{*-av_q}\beta_q(\sigma_2)>_F]_{\delta_q} \qquad \text{C. Q. F. D.}$$

On en tire

Théorème 19. $\overset{(q+1)}{V}{}^{(Z^*)}$ est un sous-hypergroupe semi-invariant de $\overset{(q)}{V}{}^{(Z^*)}$. La correspondance $\sigma \to \beta_q(\sigma)$ établit un isomorphisme de $(\overset{(p)}{V}/\overset{(q+1)}{V})^{(Z^*)}$ à l'ensemble $\bar{\alpha}^{*-av_q}\mathrm{M}_q(\mathrm{K}/k)$ organisé par la loi de composition donnée par

$$a*b=a+[<b>_F]_{\delta_q}$$

$\bar{\alpha}^{*-av_q}\mathrm{M}_q(\mathrm{K}/k)$ admet comme opérateur la transformation $\mathfrak{Z}$.

Démonstration. Analogue à celle du théorème 11.

On tire de ce théorème le

Théorème 20. Pour que $(\mathrm{A}/\overset{(q+1)}{V})^{(Z^*)}$ $(\mathrm{A}\leqq\overset{(q)}{V})$ soit un sous-hypergroupe de $(\overset{(q)}{V}/\overset{(q+1)}{V})^{(Z^*)}$ $(q\geqq 0)$, il est nécessaire et suffisant que $\bar{\alpha}^{*-av_q}.\beta_q(\mathrm{A};\pi^*,\mathfrak{P}^*)$ soit un module admettant comme opérateurs la multiplication par $\mathfrak{E}_{\bar{\delta}_q}$ et la transformation $\mathfrak{Z}$.

Démonstration. Analogue à celle de la conséquence du théorème 12.

9° Sous-corps caractéristiques de K/k pour $\mathfrak{P}$. — Si Z ou $\overset{(q)}{V}$ est un sous-hypergroupe de $G_{\mathrm{K}/k}$, il existe resp. un sous-corps $\mathrm{K}_Z^{(\mathfrak{P}^*)}$ ou $\mathrm{K}_q^{(\mathfrak{P}^*)}$ de K appartenant resp. à Z ou à $\overset{(q)}{V}$ dans K.

Définitions 3. S'il existe un sous-corps $\mathrm{K}_Z^{(\mathfrak{P}^*)}/k$ de K/k appartenant à $\mathrm{Z}_{\mathrm{K}/k}(\mathfrak{P}^*)$ dans K, il s'appelle *corps de décomposition* de $\mathfrak{P}^*$ dans K/k.

S'il existe un sous-corps $\mathrm{K}_q^{(\mathfrak{P}^*)}/k$ de K/k appartenant à $\overset{(q)}{V}_{\mathrm{K}/k}/\mathfrak{P}^*)$ dans K, il s'appelle *corps de ramification d'ordre* q *de* $\mathfrak{P}^*$ *dans* K/k $(q=1,0,1,\ldots,m)$.

En particulier, $\mathrm{K}_{-1}^{(\mathfrak{P}^*)}$ et $\mathrm{K}_0^{(\mathfrak{P}^*)}$ s'appellent, s'ils existent, resp. *corps d'inertie* et *corps de ramification* de $\mathfrak{P}^*$ dans K/k.

Je noterai $\mathfrak{p}_z$ et $\mathfrak{p}_q$ les idéaux premiers de resp. $\mathrm{K}_Z^{(\mathfrak{P}^*)}$ et $\mathrm{K}_q^{(\mathfrak{P}^*)}$ divisibles par $\mathfrak{P}^*$.

Théorème 21. Pour qu'un $K_Z^{(\mathfrak{P}^*)}/k$ ou $K_q^{(\mathfrak{P}^*)}/k$ existe il faut et il suffit que resp. $Z_{K/k}(\mathfrak{P}^*)$ ou $\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)$ soit le même pour tous les $\mathfrak{P}^*|\mathfrak{P}$.

Démonstration. Si U est un sous-hypergroupe $Z^{(Z^*)}$, on a, d'après 4° de B du chapitre I,

$$\text{gen.}_{K^*} U = \text{gen.}_{Z^*} U \cdot G_{K^*/K}.$$

Pour que cela soit un groupe il est nécessaire et suffisant, étant donné que $\text{gen.}_{Z^*} U$ et $G_{K^*/K}$ le sont, que $\text{gen.}_{Z^*} U \cdot G_{K^*/K} = G_{K^*/K} \cdot \text{gen.}_{Z^*} U$, c'est-à-dire que pour tout $\sigma^* \leqslant G_{K^*/K}$ on ait $\sigma^* U = U$.

Quand $U = Z$ ou $\overset{(q)}{V}$, c'est précisément, d'après le théorème 4, la condition de notre théorème. C. Q. F. D.

Conséquence. Si $K_Z^{(\mathfrak{P}^*)}$ ou $K_q^{(\mathfrak{P}^*)}$ existe, il est le même pour tous les $\mathfrak{P}^*|\mathfrak{P}$. On peut l'appeler corps de décomposition, resp. de ramification d'ordre q *de* $\mathfrak{P}$ *dans* K/k et désigner par $K_Z^{(\mathfrak{P})}$ ou $K_q^{(\mathfrak{P})}$.

Théorème 22. $\mathfrak{p}_Z = \mathfrak{P}^e = \mathfrak{P}^{n-1}$. $\mathfrak{p}_Z$ est d'ordre et de degré 1 dans $K_Z^{(\mathfrak{P})}/k$ et tout entier α_Z de $K_Z^{(\mathfrak{P})}$ est congru (mod $\mathfrak{p}_Z$) à un entier de k.

Démonstration. Si $K_Z^{(\mathfrak{P})}$ existe, $Z(\mathfrak{P}^*)$ est le même pour tous les $\mathfrak{P}^*|\mathfrak{P}$. Donc, si $\sigma \leqslant Z(\mathfrak{P}^*)$, la contribution de tout facteur premier dans K^*, $\mathfrak{P}^*$, de $\mathfrak{P}$ est la même dans $\mathfrak{P}$ et dans $\sigma\mathfrak{P}$. Il en résulte que $\sigma\mathfrak{P} = \mathfrak{P}$ et $N_{K/K_Z}(\mathfrak{P}) = \prod_{\sigma \leqslant Z} (\sigma\mathfrak{P})$ est une puissance de $\mathfrak{P}$. $\mathfrak{p}_Z$ qui divise $N_{K/K_Z}(\mathfrak{P})$ est aussi une puissance de $\mathfrak{P}$ dont il s'agit de déterminer l'exposant.

Pour cela remarquons que

$$Z_{K/K_Z}(\mathfrak{P}^*) = Z_{K/k}(\mathfrak{P}^*) \wedge G_{K/K_Z} = Z_{K/k}(\mathfrak{P}^*) \wedge Z_{K/k}(\mathfrak{P}^*) = Z_{K/k}(\mathfrak{P}^*)$$

et

$$T_{K/K_Z}(\mathfrak{P}^*) = T_{K/k}(\mathfrak{P}^*) \wedge G_{K/K_Z} = T_{K/k}(\mathfrak{P}^*) \wedge Z_{K/k}(\mathfrak{P}^*) = T_{K/k}(\mathfrak{P}^*).$$

Il s'ensuit que l'ordre et le degré de $\mathfrak{P}$ dans K/k et dans K/K_Z sont les mêmes. D'où $\mathfrak{p}_Z = \mathfrak{P}^e = \mathfrak{P}^{n-1}$ et est d'ordre et de degré 1 dans K_Z/k. C. Q. F. D.

Théorème 23. $\mathfrak{p} = \mathfrak{P}^{n_q}$. $\mathfrak{p}_q$ est de degré f et d'ordre $\frac{e}{n_q} = d_q$ dans $K_q^{(\mathfrak{P})}/k$. Tout entier α de K est congru (mod $\mathfrak{P}$) à un entier de $K_q^{(\mathfrak{P})}$.

Démonstration. Pour la même cause que dans le théorème 22 on a $\sigma\mathfrak{P} = \mathfrak{P}$, si $\sigma \leqslant \overset{(q)}{V}(\mathfrak{P}^*)$. Donc $\mathfrak{p}_q$ est une puissance de $\mathfrak{P}$. On a ici

$$Z_{K/K_Z}(\mathfrak{P}^*) = T_{K/K_Z}(\mathfrak{P}^*) = \overset{(q)}{V}_{K/k}(\mathfrak{P}^*),$$

donc $\mathfrak{P}$ est de degré 1 et d'ordre n_q dans K/K_q, ce qui démontre le théorème.

10° Différente de K/k. — L'idéal

$$\mathfrak{I}_{K/k} = \prod_{G'_{K/k}} (\overline{\sigma\xi - \xi}) \qquad (G'_{K/k} = G_{K/k} - \{1_k\})$$

s'appelle la *différente* de K/k. C'est un idéal du corps K. Calculons la contribution de $\mathfrak{P}$ dans $\mathfrak{I}_{K/k}$. Si σ n'est pas dans $T_{K/k}(\mathfrak{P}^*)$, $\sigma\xi - \xi$ ne se divise pas par $\mathfrak{P}^*$. Supposons que $\sigma \leqslant T_{K/k}(\mathfrak{P}^*)$ et que $\lambda_{K/k}(\sigma; \mathfrak{P}^*) = q$. La contribution de $\mathfrak{P}^*$ dans $\overline{\sigma\xi - \xi}$ est $\mathfrak{P}^{*a(1+v_q)}$. Comme dans $G'_{K/k}$ il y a $n_q - n_{q+1}$ de σ de niveau q, si $-1 \leq q < m$, et aucun σ de niveau m, l'exposant de la contribution de $\mathfrak{P}^*$ dans $\mathfrak{I}_{K/k}$ est

$$\sum_{q=-1}^{m-1} (n_q - n_{q+1}) \cdot a(1 + v_q) = a\left\{(n_{-1} - 1) + \sum_{q=0}^{m-1} (n_q - n_{q+1}) v_q\right\}$$
$$= a\left\{(n_{-1} - 1) + \sum_{q=0}^{m-1} n_q (v_q - v_{q-1}) - v_{m-1}\right\}$$

(parce que $v_{-1} = 0$ et $n_m = 1$). Donc on a le

Théorème 24. L'exposant de la contribution de $\mathfrak{P}$ dans $\mathfrak{I}_{K/k}$ est

$$e - 1 + \sum_{q=0}^{m-1} (n_q(K/k; \mathfrak{P}) - n_{q+1}(K/k; \mathfrak{P})) v_q(K/k; \mathfrak{P}) = e - 1 - v_{m-1}(K/k; \mathfrak{P})$$
$$+ \sum_{q=0}^{m-1} n_q(K/k; \mathfrak{P})(v_q(K/k; \mathfrak{P}) - v_{q-1}(K/k; \mathfrak{P}))\ (12).$$

(12) La différence de cet exposant et de $e - 1$, c'est-à-dire $\sum_{q=0}^{m-1} (n_q - n_{q+1}) v_q$, est ce que MM. Hensel et Ore appellent « le nombre supplémentaire » (« Supplementzahl »).

B. — CORPS LOCAUX

1° Isomorphismes des corps locaux. — Soit k un corps de nombres algébriques, $K^* > K > k$, K^*/k étant galoisienne.

Considérons un automorphisme de $K^*(\mathfrak{P}^*)/k(\mathfrak{p})$. Comme $K^* < K^*(\mathfrak{P}^*)$, cet automorphisme produit un isomorphisme de K^*. D'autre part, il laisse invariants les éléments de k. Il donne donc un isomorphisme de K^*/k, et, puisque K^*/k est galoisienne, un automorphisme de K^*/k.

Nous pouvons, par conséquent, faire correspondre à tout automorphisme de $K^*(\mathfrak{P}^*)/k(\mathfrak{p})$ un automorphisme de K/k. Il est évident que cette correspondance conserve la multiplication (dans les groupes). D'autre part, il est évident que si un automorphisme de $K^*(\mathfrak{P}^*)/k(\mathfrak{p})$ laisse invariants les nombres de $K^*(\mathfrak{P}^*)$, il laisse aussi invariants ceux de K^* : c'est l'automorphisme identique. Notre correspondance est donc un isomorphisme du groupe de Galois de $K^*(\mathfrak{P}^*)/k(\mathfrak{p})$ avec un sous-groupe g du groupe de Galois de K^*/k.

Les éléments de g laissent $\mathfrak{P}^*$ invariant. En effet, un élément π de $\mathfrak{P}^*$ est caractérisé par la propriété suivante : on a $\lim_{n\to+\infty} \pi^n = 0$, propriété qui est évidemment conservée par tout automorphisme de $K^*(\mathfrak{P}^*)$. Donc g est contenu dans le groupe de décomposition Z^* de $\mathfrak{P}^*$ dans K/k.

Inversement, soit $\sigma^* \leqslant Z^*$. On a $\sigma^*\mathfrak{P}^* = \mathfrak{P}^*$. Tout nombre α de $K^*(\mathfrak{P}^*)$ est la limite ($\mathfrak{P}^*$ — adique) d'une suite de nombres α_n de K^*. Comme σ^* conserve $\mathfrak{P}^*$, la suite de $\sigma^*\alpha_n$ est encore convergente. Soit $\sigma^*\alpha$ sa limite (elle ne dépend que de α). La correspondance $\alpha \to \sigma^*\alpha$ conserve évidemment l'addition et la multiplication dans $K^*(\mathfrak{P}^*)$. De plus, si une suite de nombres α_i de $K^*(\mathfrak{P}^*)$ tend vers 0, il en est de même de la suite des $\sigma^*\alpha_i$. Donc $\alpha \to \sigma^*\alpha$ est un automorphisme de $K^*(\mathfrak{P}^*)/k(\mathfrak{p})$ et cet automorphisme produit σ^* dans K^*. Donc σ^* est dans g et l'on a $Z^* = g$.

Soit maintenant K une extension de k contenue dans K^*. L'isomorphisme précédent fait correspondre le groupe $Z_{K^*/K}(\mathfrak{P}^*)$ avec $G_{K^*(\mathfrak{P}^*)/K(\mathfrak{p})}$. Or, l'hypergroupe de décomposition Z de $\mathfrak{P}^*$ dans K/k (avec la loi de composition qui y est induit par Z^*) n'est autre que le quotient $Z^*/Z_{K^*/K}$. Notre correspondance établit donc un isomorphisme entre Z et l'hypergroupe quotient

$G_{K^*(\mathfrak{P}^*)/k(\mathfrak{p})}/G_{K^*(\mathfrak{P}^*)/K(\mathfrak{P})}$. Ce dernier hypergroupe est isomorphe à $G_{K(\mathfrak{P})/k(\mathfrak{p})}$, l'isomorphisme étant établi par

$$\sigma^* \to \text{corr.}_{K(\mathfrak{P})}\, \sigma^* \quad (\sigma^* \leqslant G_{K^*(\mathfrak{P}^*)/k(\mathfrak{p})}).$$

Donc

L'hypergroupe de décomposition de $\mathfrak{P}^*$ dans K/k est isomorphe à l'hypergroupe de Galois de $K(\mathfrak{P})/k(\mathfrak{p})$.

De plus, l'isomorphisme indiqué fait correspondre aux éléments T, $\overset{(q)}{V}$ de la suite caractéristique de $\mathfrak{P}^*$ dans K/k des sous-ensembles de l'hypergroupe $G_{K(\mathfrak{P})/k(\mathfrak{p})}$ qui, en vertu du théorème 4, sont des sous-hypergroupes de l'hypergroupe de Galois. Ces ensembles sont appelés *hypergroupe d'inertie* et *hypergroupes de ramification* (d'ordre q) dans $K(\mathfrak{P})/k(\mathfrak{p})$.

Les sous-corps de $K(\mathfrak{P})/k(\mathfrak{p})$ qui appartiennent à ces hypergroupes sont appelés resp. *corps d'inertie* et *corps de ramification d'ordre q* de $K(\mathfrak{P})/k(\mathfrak{p})$.

On peut encore définir directement, exactement comme pour les corps de nombres algébriques, ces notions ainsi que celle de nombre caractéristique et des nombres de ramification. On montre facilement qu'on arrive ainsi aux mêmes ensembles et que les éléments correspondants de Z et de $G_{K(\mathfrak{P})/k(\mathfrak{p})}$ ont les mêmes $v(\sigma; \mathfrak{P}^*)$ et, éventuellement, les mêmes $i_k(\sigma; \mathfrak{P}^*)$, $\beta_{-1}(\sigma; \mathfrak{P}^*)$, $\beta_q(\sigma; \pi^*, \mathfrak{P}^*)$.

Dans la notation des symboles qui expriment les notions en question on n'a pas, dans le cas local, à indiquer l'idéal $\mathfrak{P}^*$ ou $\mathfrak{P}$, puisqu'il n'y en a qu'un seul.

Tous les résultats démontrés dans la partie A de ce chapitre s'étendent aux corps de nombres $\mathfrak{P}$ — adiques, mais certains d'entre eux deviennent triviaux dans le cas local (par exemple, théorème 21).

2° Primitivité des corps locaux. — On appelle *primitif* un corps K/k tel qu'il n'existe aucun corps, contenu dans K et contenant k, autre que K ou k.

Soient k un corps local de degré fini, K une extension finie de K/k.

Théorème 1. La condition nécessaire et suffisante pour que K/k soit primitif est que ou bien K/k soit degré premier, ou bien K/k soit complètement ramifiée de degré puissance de p, n'ait qu'un seul nombre de ramification propre $v = v_0\,(K/k)$ et soit tel que, δ étant le plus grand facteur premier à p du déno-

minateur δ de v et f_0 étant le degré absolu de l'idéal premier $\mathfrak{p}$ de k dans k, $\mathrm{M}(\mathrm{K}/k) = \mathrm{M}(\mathrm{K}/k; \sqrt[\delta]{\pi})$ (où π est un nombre de K d'ordre 1 en $\mathfrak{P}$) n'ait de sous-modules $\overline{\mathrm{M}}$, tels que $[<\overline{\mathrm{M}}>_{f_0}]_\delta = \overline{\mathrm{M}}$, autres que $\mathrm{M}(\mathrm{K}/k)$ lui-même et $\{0\}$.

Démonstration. On a vu que tous les corps caractéristiques K_q/k de K/k existent ($q = -1, 0, 1, \ldots, m$).

Soit n le moindre entier tel que $\mathrm{K}_n \neq k$. Certainement $n \leqq 1$. Si $m > n$, K_n est un corps intermédiaire entre K et k et inégal à aucun d'eux et K/k n'est pas primitif. Donc, si K/k est primitif, on a $m = n$ et $m \leqq 1$. Il se présente trois cas :

a) $m = -1$. Dans ce cas $G_{\mathrm{K}/k} = \mathrm{Z}_{\mathrm{K}/k}$ et $\mathrm{T}_{\mathrm{K}/k} = 1$. Donc $G_{\mathrm{K}/k} \simeq \mathrm{Z}_{\mathrm{K}/k}/\mathrm{T}_{\mathrm{K}/k}$ est un groupe et K/k est Galoisien. Il n'est primitif que si $(\mathrm{K} : k)$ est premier;

b) $m = 0$. Dans ce cas, puisque $n = m$, on doit avoir $\mathrm{K}_{-1} = k$, $\mathrm{K}_0 = \mathrm{K}$. Donc $G_{\mathrm{K}/k} \simeq \mathrm{T}_{\mathrm{K}/k}/\mathrm{V}_{\mathrm{K}/k}$. D'après la conséquence du théorème 11 de A de ce chapitre, la condition nécessaire et suffisante pour que $\mathrm{A}/\mathrm{V}_{\mathrm{K}/k}$ soit un sous-hypergroupe de $\mathrm{T}_{\mathrm{K}/k}/\mathrm{V}_{\mathrm{K}/k}$ est que $\beta_{-1}(\mathrm{A})$ soit groupe multiplicatif. Donc, pour que K/k soit primitif il faut et il suffit que $\mathrm{M}_{-1}(\mathrm{K}/k)$ n'ait d'autres sous-groupes multiplicatifs que lui-même et $\{1\}$, c'est-à-dire soit de degré premier, c'est-à-dire que $(\mathrm{K} : k)$ soit premier;

c) $m = 1$. Dans ce cas on doit avoir $\mathrm{K}_0 = k$, $\mathrm{K}_1 = \mathrm{K}$; K/k est bien complètement ramifié de degré puissance de p et n'ayant qu'un seul nombre de ramification propre. De plus, $\mathrm{F} = f_0$ et $G_{\mathrm{K}/k} \simeq \overset{(0)}{\mathrm{V}}_{\mathrm{K}/k}/\overset{(1)}{\mathrm{V}}_{\mathrm{K}/k}$. Pour que $\mathrm{A}/\overset{(1)}{\mathrm{V}}_{\mathrm{K}/k}$ soit un sous-hypergroupe de $\overset{(0)}{\mathrm{V}}_{\mathrm{K}/k}/\overset{(1)}{\mathrm{V}}_{\mathrm{K}/k}$, il faut et il suffit, d'après théorème 20 de A de ce chapitre, que $\beta_0(\mathrm{K}/k; \sqrt[\delta]{\pi})$ satisfasse à la condition de l'énoncé (on vérifie facilement qu'ici $\bar{\alpha}^* = 1$), ce qui achève la démonstration.

J'ai consacré à la question de primitivité de corps locaux un travail, dont la première partie doit paraître cette année au tome XIII du journal *Matematica*.

J'y mets la condition pour le cas *c*) sous deux formes très curieuses, à l'aide de certaines expressions symboliques.

3° Développement d'un élément local en séries de puissances fractionnaires d'un autre élément local d'ordre positif. — J'ai besoin de faire ici une étude brève de cette question à cause d'une démonstration du chapitre IV. Soient donc

α un élément local et π un autre élément local d'ordre positif. J'appelle *développement normal* de α suivant π l'expression de α sous forme d'une série locale

$$\alpha = \sum_{q=0}^{+\infty} \rho_q \pi^{u_q}$$

où les ρ_q sont des racines de l'unité (locales) d'ordre premier au nombre premier p du corps local rationnel et les u_q sont des fractions rationnelles croissantes avec q et tels que $\lim_{q \to +\infty} u_q = +\infty$. Il est évident que si un développement normal de α suivant π existe, il est unique. Il s'agit d'en prouver l'existence dans un cas particulier. Pour cela on a besoin du lemme suivant :

Lemme 1. Si un polynôme $f(x)$ est irréductible dans un corps local k, $\mathfrak{p}$ étant l'idéal premier de ce corps, le polynôme $f(x)$ ne peut pas se décomposer (mod $\mathfrak{p}$) en deux facteurs premiers entre eux (mod $\mathfrak{p}$).

Démonstration. Supposons que $f(x) \equiv g(x)\, h(x) \pmod{\mathfrak{p}}$ et que $g(x)$, $h(x)$ sont premiers entre eux (mod $\mathfrak{p}$). Supposons plus généralement que cela a lieu (mod $\mathfrak{p}^n$) et que le coefficient de la plus grande puissance de x dans $f(x)$ est égal au produit des tels coefficients dans $g(x)$ et $h(x)$. Posons, π étant un nombre de k d'ordre 1 en $\mathfrak{p}$,

$$g'(x) = g(x) + \pi^n g_1(x); \qquad h'(x) = h(x) + \pi^n h_1(x).$$

On a

$$h'(x)\, g'(x) \equiv g(x)\, h(x) + \pi^n (g_1(x)\, h(x) + h_1(x)\, g(x)) \equiv f(x)$$
$$+ \pi^n \left\{ \frac{g(x)\, h(x) - f(x)}{\pi^n} + g_1(x)\, h(x) + h_1(x)\, g(x) \right\} \pmod{\mathfrak{p}^{n+1}}.$$

Or $\dfrac{g(x)\, h(x) - f(x)}{\pi^n}$ est un polynôme de degré moindre que celui de $g(x)\, h(x)$ et à coefficients entiers. $g(x)$, $h(x)$ étant premiers (mod $\mathfrak{p}$), on peut trouver $g_1(x)$ de degré moindre que celui de $g(x)$ et $h_1(x)$ de degré moindre que celui de $h(x)$ tels que

$$\frac{g(x)\, h(x) - f(x)}{\pi^n} + g_1(x)\, h(x) + h_1(x)\, g(x) \equiv 0 \pmod{\mathfrak{p}}$$

et alors

$$f(x) \equiv g'(x)\, h'(x) \pmod{\mathfrak{p}^{n+1}}$$

et

$$g'(x) \equiv g(x), \qquad h'(x) \equiv h(x) \pmod{\mathfrak{p}^{n+1}}.$$

Par le même procédé on obtient à partir de $g'(x)$, $h'(x)$ les polynômes $g''(x)$, $h''(x)$, etc.

Les suites $g(x)$, $g'(x)$, $g''(x)$, ... et $h(x)$, $h'(x)$, $h''(x)$, ... sont convergentes par rapport aux coefficients; si $g(x)$, $h(x)$ sont leurs limites, on a

$$f(x) = g(x)\,h(x). \qquad \text{C. Q. F. D.}$$

Théorème 2. Si K/k n'a qu'un seul nombre de ramification propre, il existe un développement normal de tout conjugué par rapport à K_0 $\sigma\pi$ d'un nombre π de K d'ordre 1 en $\mathfrak{P}$ suivant π.

Démonstration. δ étant le dénominateur de $v = v_0(K/k)$, considérons l'équation dans $K(\sqrt[\delta]{\pi})$ à laquelle satisfont les $\frac{\sigma\pi - \pi}{\pi(\sqrt[\delta]{\pi})^{\delta v}}$ non nuls ($\sigma \leqslant V_{K/k}$).

Cette équation a toutes ses racines incongrues deux à deux (mod $\mathfrak{P}^*$). Si l'on adjoint à $K(\sqrt[\delta]{\pi})$ des racines de l'unité d'ordre premier à p congrues à ces nombres (mod $\mathfrak{P}^*$), on obtient un corps K' dont l'idéal premier est $(\sqrt[\delta]{\pi})$, et où l'équation regardée, en vertu du lemme précédent, se décompose complètement. Donc tous les $\sigma\pi$ appartiennent à K', et comme chaque nombre de K' se met sous la forme d'un développement normal suivant $\sqrt[\delta]{\pi}$, donc suivant π; le théorème est démontré.

CHAPITRE III

ÉTUDE DES CORPS INTERMÉDIAIRES

A. — ÉTUDE DU SOUS-CORPS A PARTIR DU CORPS ET DU CORPS RELATIF

1° Notation. — Soit $K > \overline{K} > k$ (k étant un corps de nombres algébriques ou un corps local de degré fini). Désignons

$v_q(\mathfrak{P}; K/k)$, $n_q(\mathfrak{P}; K/k)$, $r_q(\mathfrak{P}; K/k)$ resp. par v_q, n_q, r_q.

$v_q(\overline{\mathfrak{P}}; \overline{K}/k)$, $n_q(\overline{\mathfrak{P}}; \overline{K}/k)$, $r_q(\overline{\mathfrak{P}}; \overline{K}/k)$ resp. par $\overline{v_q}$, $\overline{n_q}$, $\overline{r_q}$. ($\overline{\mathfrak{P}}$ désigne l'idéal premier de $\overline{K}$ divisible par $\mathfrak{P}$).

$v_q(\mathfrak{P}; K/\overline{K})$, $n_q(\mathfrak{P}; K/\overline{K})$, $r_q(\mathfrak{P}; K/K)$ resp. par w_q, ν'_q, ρ'_q.

$z(\mathfrak{P}; K/k)$, $z(\overline{\mathfrak{P}}; \overline{K}/k)$, $z(\mathfrak{P}; K/\overline{K})$ resp. par z, $\overline{z}$, ξ.

On pose

$$v_m = \overline{v}_{\overline{m}} = w_\mu = +\infty$$

$$\overset{(q)}{\nu} = \overset{(q)}{V}_K \wedge G_{K/\overline{K}}, \qquad \nu_q \text{ nombre d'éléments de } \overset{(q)}{\nu}, \qquad \rho_q = \frac{\nu_q}{\nu_{q+1}}, \quad \Delta_q = \frac{\nu_{-1}}{\nu_q}.$$

Soient

$$0 \leqq \varepsilon_0(\mathfrak{P}; K, \overline{K}, k) < \varepsilon_1(\mathfrak{P}; K, \overline{K}, k) < \cdots < \varepsilon_{s'-1}(\mathfrak{P}; K, \overline{K}, k) \leqq m-1$$

l'ensemble de tous les q, $0 \leqq q \leqq m-1$, tels que $\rho_q \neq 1$, et

$$0 \leqq i_0(\mathfrak{P}; K, \overline{K}, k) < i_1(\mathfrak{P}; K, \overline{K}, k) < \cdots < i_{s''-1}(\mathfrak{P}; K, \overline{K}, k) \leqq m-1$$

l'ensemble de tous les q, $0 \leqq q \leqq m-1$, tels que $\rho_q \neq r_q$.

On pose

$$\varepsilon_{-1}(\mathfrak{P}; K, \overline{K}, k) = i_{-1}(\mathfrak{P}; K, \overline{K}, k) = -1; \quad \varepsilon_{s'}(\mathfrak{P}; K, \overline{K}, k) = i_{s''}(\mathfrak{P}; K, \overline{K}, k) = m.$$

2° Corps relatifs. — On a un théorème qui était déjà employé implicitement dans les cas simples :

Théorème 1.

$$Z_{K/\overline{K}}(\mathfrak{P}^*) = Z_K(\mathfrak{P}^*) \wedge G_{K/\overline{K}}; \quad \mu = s'; \quad \overset{(q)}{V}_{K/\overline{K}}(\mathfrak{P}^*) = \overset{(\varepsilon_{q-1}+1)}{\nu} = \overset{(\varepsilon_{q-1}+2)}{\nu} = \cdots = \overset{(\varepsilon_q)}{\nu};$$

$$\nu'_q = \nu_{\varepsilon_{q-1}+1} = \nu_{\varepsilon_{q-1}+2} = \cdots = \nu_{\varepsilon_q}; \qquad w_q = v_{\varepsilon_q} \qquad (q = -1, 0, 1, \ldots, \mu).$$

Démonstration. Par définition, $Z_{K/\overline{K}}(\mathfrak{P}^*) = Z_K(\mathfrak{P}^*) \wedge G_{K/\overline{K}}$, $T_{K/\overline{K}}(\mathfrak{P}^*) = T_K(\mathfrak{P}^*) \wedge G_{K/\overline{K}}$ et les $\overset{(q)}{V}_{K/\overline{K}}(\mathfrak{P}^*)$ sont les ensembles distincts de la suite des $\overset{(q')}{\nu} = \overset{(q')}{V}_K(\mathfrak{P}^*) \wedge G_{K/\overline{K}}$; or, $\overset{(q')}{\nu}$ est $=$ ou $\neq \overset{(q'+1)}{\nu}$, suivant que $\rho_{q'} =$ ou $\neq 1$, c'est-à-dire suivant que q' est différent de tous les ε_q ou qu'il est égal à l'un d'eux, ce qui démontre le théorème.

3° Étude des sous-corps. — On a vu que

$$\left.\begin{aligned} Z_{\overline{K}}(\mathfrak{P}^*) &= \text{corr.}_{\overline{K}}\, Z_K(\mathfrak{P}^*) \qquad \text{(th. 6 de A du chap. II)} \\ T_{\overline{K}}(\mathfrak{P}^*) &= \text{corr.}_{\overline{K}}\, T_K(\mathfrak{P}^*) \\ V_{\overline{K}}(\mathfrak{P}^*) &= \text{corr.}_{\overline{K}}\, V_K(\mathfrak{P}^*) \end{aligned}\right\} \text{(th. 10 de A du chap. II).}$$

Les deux derniers résultats sont les cas les plus simples du théorème général suivant :

Théorème 2.

$$\overline{m} = s''; \quad \overset{(q)}{V}_{\overline{K}}(\mathfrak{P}^*) = \text{corr.}_{\overline{K}}\, \overset{(i_{q-1}+1)}{V}_K(\mathfrak{P}^*) = \text{corr.}_{\overline{K}}\, \overset{(i_{q-1}+2)}{V}_K(\mathfrak{P}^*) = \cdots = \text{corr.}_{\overline{K}}\, \overset{(i_q)}{V}_K(\mathfrak{P}^*)\ (^1)$$

$$(1) \qquad \overline{v}_q = \sum_{s=0}^{i_q} \frac{v_s - v_{s-1}}{\Delta_s} \qquad (q = -1, 0, 1, \ldots, \overline{m})\ (^1).$$

(1) Il suit de ce théorème que

$$\text{gen.}_K\, Z_{\overline{K}} = Z_K G_{K/\overline{K}}, \qquad \text{gen.}_K\, T_{\overline{K}} = T_K G_{K/\overline{K}},$$

et que les $\text{gen.}_K\, \overset{(q)}{V}_{\overline{K}}$ sont les ensembles distincts de la suite des $\overset{(q)}{V}_K G_{K/\overline{K}}$. Dedekind, pour étudier un sous-corps non-galoisien $\overline{K}$ d'un corps galoisien K intoduisit les ensembles $G_{K/\overline{K}} Z_K$ et $G_{K/\overline{K}} T_K$ (qui pourraient se généraliser par les $G_{K/\overline{K}} \overset{(q)}{V}_K$).

Ces ensembles ont le même nombre d'éléments que resp. $\text{gen.}_K\, Z_{\overline{K}}$, $\text{gen.}_K\, T_{\overline{K}}$, et les $\text{gen.}_K\, \overset{(q)}{V}_{\overline{K}}$ correspondants et, par ex., le quotient du nombre d'éléments de $G_{K/\overline{K}} Z_K$ par l'ordre de $G_{K/\overline{K}}$ est $\bar{e}\bar{f}$, celui du nombre d'éléments de $G_{K/K} T_K$ par l'ordre de $G_{K/\overline{K}}$ est $\bar{e}$. Mais ces ensembles n'ont pas de signification intrinsèque dans $\overline{K}$ et ne

Démonstration. Considérons l'hypergroupe de K/k. Posons $\overset{(q)}{W} = \overset{(q)}{V}_K G_{K/\overline{K}}$. $\bar{\sigma} \neq 1_{\overline{K}}$ étant un élément arbitraire de $T_{\overline{K}} = \text{corr.}_{\overline{K}}\ T_K$, on peut trouver un q, $-1 \leq q \leq m-1$, tel que $\text{gen.}_K \bar{\sigma}$ (qui est une classe suivant $G_{K/\overline{K}}$, d'après 3° de B du chapitre I) soit contenu dans $\overset{(q)}{W}$ et disjoint avec $\overset{(q+1)}{W}$. Alors $\text{gen.}_K \bar{\sigma}$ a des éléments communs avec $\overset{(q)}{V}_K$ et n'en a pas avec $\overset{(q+1)}{V}_K$. Par conséquent, puisque tous les $\overset{(s)}{V}{}_K^{(Z^*)}$ $(s = -1, 0, 1, \ldots, m)$ sont hypergroupes, en vertu du 4° de B de chapitre I, le nombre d'éléments de $\text{gen.}_K \bar{\sigma} \wedge \overset{(s)}{V}_K$ est égal à celui de $G_{K/\overline{K}} \wedge \overset{(s)}{V}_K = \overset{(s)}{\nu}$, c'est-à-dire est ν_s si $-1 \leq s \leq q$, et est 0 si $q < s \leq m$.

D'après le théorème 40 de Hilbert le contenu de $\bar{\sigma}\bar{\xi} - \bar{\xi}$ ($\bar{\xi}$ étant une forme fondamentale de $\overline{K}$) est égal à celui de $\prod_{\sigma \leqslant \text{gen.}_K \bar{\sigma}} (\sigma\xi - \xi)$ (ξ étant une forme fondamentale de K). Comme $\text{gen.}_K \bar{\sigma}$ contient, d'après ce qui précède, $\nu_{-1} - \nu_0$ éléments de niveau -1, $\nu_0 - \nu_1$ éléments de niveau 0, $\nu_1 - \nu_2$ éléments de niveau 1, ..., $\nu_{q-1} - \nu_q$ éléments de niveau $q-1$, ν_q éléments de niveau q, et aucun élément de niveau supérieur, l'ordre en $\mathfrak{P}^*$ du contenu de $\bar{\sigma}\bar{\xi} - \bar{\xi}$, $\mathfrak{P}^{*a}$ étant, comme au chapitre II, la contribution de $\mathfrak{P}^*$ dans $\mathfrak{P}$, est

$$a\left\{\left(\sum_{s=0}^{q}(\nu_{s-1}-\nu_s)(1+v_{s-1})\right)+\nu_q(1+v_q)\right\}$$

$$= a\left\{\left(\sum_{s=0}^{q}(\nu_{s-1}-\nu_s)\right)+\nu_q+\left(\sum_{s=0}^{q}(\nu_{s-1}-\nu_s)v_{s-1}\right)+v_q\nu_q\right\}$$

$$= a\nu_{-1} + a\left(\nu_{-1}v_{-1} + \sum_{s=0}^{q}\nu_s(v_s - v_{s-1})\right) = a\nu_{-1}\left\{1 + \sum_{s=0}^{q}\frac{v_s - v_{s-1}}{\Delta_s}\right\}$$

car

$$v_{-1} = 0 \qquad \text{et} \qquad \frac{\nu_s}{\nu_{-1}} = \frac{1}{\Delta_s}.$$

Or $\nu_{-1} = n_{-1}(K/\overline{K}; \mathfrak{P})$ étant égal (th. 9 du ch. II) à l'ordre de $\mathfrak{P}$ par rapport à $\overline{K}$, $\mathfrak{P}^{a\nu_{-1}}$ est la contribution de $\mathfrak{P}^*$ dans l'idéal premier $\overline{\mathfrak{P}}$ de $\overline{K}$ qu'il divise et

---

permettent pas de définir les nombres de ramification et les ensembles $M_q(\overline{K}/k)$. Pour cette cause je les considère comme mal appropriés à la nature du problème. $G_{K/\overline{K}} Z_K$, $G_{K/\overline{K}} \overset{(i_q)}{V}_K$ coïncide avec resp. $\text{gén.}_K Z_{\overline{K}} = Z_K G_{K/\overline{K}}$, $\text{gén.}_K \overset{(q)}{V}_{\overline{K}} = \overset{(i_q)}{V}_K G_{K/\overline{K}}$ quand il est un groupe, c'est-à-dire quand il existe resp. $\overline{K}_z/k$, $\overline{K}_q/k$. $G_{K/\overline{K}} Z_K$ est l'ensemble de tous les $\sigma \leqslant G_{K/\overline{K}}$ tels que $\sigma\mathfrak{P}$ divise $\overline{\mathfrak{P}}$.

l'expression précédente est, ainsi, égale à $a v_{-1}[1 + v(\bar{\sigma}; \mathfrak{P}^*)]$. Il en résulte que

$$v(\bar{\sigma}; \mathfrak{P}^*) = \sum_{s=0}^{q} \frac{v_s - v_{s-1}}{\Delta_s}.$$

Pour qu'il existe un $\bar{\sigma} \leqslant \mathrm{V}_{\bar{\mathrm{K}}}$ tel que

$$v(\bar{\sigma}; \mathfrak{P}^*) = \sum_{s=0}^{q'} \frac{v_s - v_{s-1}}{\Delta_s} \quad (0 \leqq q' \leqq m-1)$$

il est nécessaire et suffisant que $\mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(q')}{\mathrm{W}} \neq \mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(q'+1)}{\mathrm{W}}$; or, le nombre d'éléments de $\mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(q')}{\mathrm{W}} = \mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(q')}{\mathrm{V}}_{\mathrm{K}}$ est égal, d'après 4° de B du chapitre I, puisque $\overset{(q')}{\mathrm{V}}_{\mathrm{K}}^{(Z^*)}$ est hypergroupe, à celui de $\left(\overset{(q')}{\mathrm{V}}_{\mathrm{K}} / (\overset{(q')}{\mathrm{V}}_{\mathrm{K}} \wedge G_{\mathrm{K}/\bar{\mathrm{K}}})\right)^{(Z^*)}$, c'est-à-dire à $\frac{n_{q'}}{\nu_{q'}}$, et de même le nombre d'éléments de $\mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(q'+1)}{\mathrm{W}}$ est égal à $\frac{n_{q'+1}}{\nu_{q'+1}}$; donc, $\mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(q')}{\mathrm{W}} =$ ou $\neq \mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(q'+1)}{\mathrm{W}}$ suivant que $\frac{n_{q'}}{\nu_{q'}} =$ ou $\neq \frac{n_{q'+1}}{\nu_{q'+1}}$, c'est-à-dire suivant que $r_q = \frac{\nu_q}{\nu_{q+1}} =$ ou $\neq \frac{\nu_q}{\nu_{q+1}} = \rho_q$, c'est-à-dire suivant que q' ne se trouve pas ou se trouve parmi les nombres $i_0, i_1, \ldots, i_{s''-1}$. Donc, l'ensemble des nombres caractéristiques des $\sigma \leqslant \mathrm{V}_{\bar{\mathrm{K}}}$ est

$$0 < \sum_{s=0}^{i_0} \frac{v_s - v_{s-1}}{\Delta_s} < \sum_{s=0}^{i_1} \frac{v_s - v_{s-1}}{\Delta_s} < \cdots < \sum_{s=0}^{i_{s''-1}} \frac{v_s - v_{s-1}}{\Delta_s} < +\infty = \sum_{s=0}^{i_{s''}} \frac{v_s - v_{s-1}}{\Delta_s}$$

Cela démontre la partie du théorème relative aux nombres de ramification et démontre aussi que $\overset{(q)}{\mathrm{V}}_{\bar{\mathrm{K}}} = \mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(i_q)}{\mathrm{V}}_{\mathrm{K}}$. Puisque

$$r_{i_{q-1}+1} - \rho_{i_{q-1}+1} = r_{i_{q-1}+2} - \rho_{i_{q-1}+2} = \cdots = r_{i_q - 1} - \rho_{i_q - 1} = 0,$$

on a

$$\mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(i_{q-1}+1)}{\mathrm{V}}_{\mathrm{K}} = \mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(i_{q-1}+2)}{\mathrm{V}}_{\mathrm{K}} = \cdots = \mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(i_q - 1)}{\mathrm{V}}_{\mathrm{K}} = \mathrm{corr.}_{\bar{\mathrm{K}}} \overset{(i_q)}{\mathrm{V}}_{\mathrm{K}}$$

et le théorème est démontré.

Définition. On dira que v_{i_q} est le nombre de ramification de $\mathfrak{P}$ dans K/k qui *engendre* $\bar{v}_q$.

Autre expression du même théorème. Soit t_q l'entier tel que

$$w_{i_q} \leqq v_{i_q} < w_{i_q+1} \qquad (q = -1, 0, 1, \ldots, \overline{m}). \tag{2}$$

Désignons par Δ'_q $(q = 1, 0, \ldots, \mu)$ le nombre $\frac{\nu'_{-1}}{\nu'_q} = \frac{\nu_{-1}}{\nu'_q}$. On a

$$\Delta_{\varepsilon_{q-1}+1} = \Delta_{\varepsilon_{q-1}+2} = \cdots = \Delta_{\varepsilon_q} = \Delta'_q.$$

Il s'ensuit

$$\sum_{s=0}^{i_q}\frac{v_s-v_{s-1}}{\Delta_s}=\sum_{s=\varepsilon_{t_q}+1}^{i_q}\frac{v_s-v_{s-1}}{\Delta_s}+\sum_{j=0}^{t_q}\sum_{s=\varepsilon_{j-1}+1}^{\varepsilon_j}\frac{v_s-v_{s-1}}{\Delta_s}=\frac{1}{\Delta'_{t_q+1}}\sum_{s=\varepsilon_{t_q}+1}^{i_q}(v_s-v_{s-1})$$

$$+\sum_{j=0}^{t_q}\sum_{s=\varepsilon_{j-1}+1}^{\varepsilon_j}\frac{v_s-v_{s-1}}{\Delta'_j}=\frac{v_{i_q}-v_{\varepsilon_{t_q}}}{\Delta'_{t_q+1}}+\sum_{j=0}^{t_q}\frac{v_{\varepsilon_j}-v_{\varepsilon_{j-1}}}{\Delta'_j}=\frac{v_{i_q}-w_{t_q}}{\Delta'_{t_q+1}}+\sum_{j=0}^{t_q}\frac{w_j-w_{j-1}}{\Delta'_j}.$$

D'où il résulte que

$$\bar{v}_q=\frac{v_{i_q}-w_{t_q}}{\Delta'_{t_q+1}}+\sum_{j=0}^{t_q}\frac{w_j-w_{j-1}}{\Delta'_j}\qquad(q=-1,0,1,\ldots,\overline{m}).\tag{3}$$

Théorème 3.

$$\bar{z}=\frac{z}{\varsigma};\quad \bar{n}_q=\frac{n_{i_{q-1}+1}}{\nu_{i_{q-1}+1}}=\frac{n_{i_{q-1}+2}}{\nu_{i_{q-1}+2}}=\cdots=\frac{n_{i_q}}{\nu_{i_q}};\quad \bar{r}_q=\frac{r_q}{\rho_{i_q}}.$$

Démonstration. D'après 4° de la partie B du chapitre I, le nombre d'éléments de corr.$_{\overline{K}}$ Z_K ou corr.$_K$ $\overset{(q)}{V}_K$ $(q=1, 0, 1, \ldots, m)$ est égal à celui de resp. $(Z_K/(Z_K\wedge G_{K|\overline{K}}))^{(Z^*)}=(Z_K/Z_{K/\overline{K}})^{(Z^*)}$ ou $(\overset{(q)}{V}_K/(\overset{(q)}{V}_K\wedge G_{K|\overline{K}}))^{(Z^*)}=(\overset{(q)}{V}_K/\overset{(q)}{\nu})^{(Z^*)}$, c'est-à-dire à $\frac{z}{\xi}$ et $\frac{n_q}{\nu_q}$, ce qui démontre le théorème.

Dans le cas où K/k et $\overline{K}/k$ sont Galoisiens, le théorème équivalent aux théorèmes 2 et 3 fut démontré par Jacques Herbrand dans son travail « Contribution à la théorie des groupes de décomposition, d'inertie et de ramification », paru dans *Journal des Mathématiques pures et appliquées*, 1931, pp. 481-498. Toutefois, la forme que Herbrand a donnée à son théorème est peu commode (en particulier, son théorème ne détermine qu'implicitement les $\bar{v}_q$ à partir des v_q et des ν_q). C'est M. Helmut Hasse qui a mis (à la fin de sa deuxième note sur les restes normiques dans les *Comptes rendus* de 1933) le résultat de Herbrand sous la forme qui ne diffère du théorème 2 que par une petite différence de notation. Il est à remarquer que le théorème sous la forme de Herbrand n'est vrai pour K/k, $\overline{K}/k$ non-Galoisiens que si tous les $v_q(q=-1, 0, 1, \ldots, m-1)$ et $\bar{v}_q(=-1, 0, 1, \ldots \ldots, \overline{m}-1)$ sont entiers. Par contre, sous la forme de Hasse, il devient dans le cas général le théorème 2 de ce chapitre.

La démonstration de Herbrand est tout à fait analogue à celle du théorème 2. Toutefois, dans le cas non-Galoisien, certains points, triviaux dans

le cas Galoisien : détermination du nombre d'éléments de $\text{gen.}_K \bar{\sigma} \wedge \overset{(q)}{V}_K$ et de celui de $\text{corr.}_{\bar{K}} \overset{(q)}{W}$ — deviennent délicats, et, comme on a vu, exigent l'emploi de certains résultats sur les hypergroupes, et (point essentiel!) du théorème que $Z_K^{(Z^*)}$ et les $\overset{(q)}{V}{}_K^{(Z^*)}$ sont hypergroupes.

Théorème 4. Si $\bar{\sigma} = \overset{\circ}{\text{corr.}}_{\bar{K}} \sigma\,[\sigma \leqslant Z_K(\mathfrak{P}^*)]$ et si $\bar{f}$ est le degré de $\bar{\mathfrak{P}}$ dans $\bar{K}/k$, on a

$$i_k(\sigma) \equiv i_k(\bar{\sigma}) \pmod{\bar{f}}. \tag{4}$$

Démonstration. $\bar{n}$ désignant la norme absolue de $\mathfrak{p}$ dans k et i étant dans $i(\sigma)$, on a pour tout entier α de K

$$\sigma\alpha \equiv \alpha^{\bar{n}^i} \pmod{\mathfrak{P}^*}. \tag{5}$$

En particulier, pour tout entier $\bar{\alpha}$ de $\bar{K}$ on a

$$\bar{\sigma}\bar{\alpha} \equiv \bar{\alpha}^{\bar{n}^i} \pmod{\mathfrak{P}^*}, \tag{6}$$

ce qui démontre le théorème.

Conséquence. Si $e = 1$, $\left(\dfrac{\bar{K}/k}{\mathfrak{P}^*}\right) = \text{corr.}_{\bar{K}} \left(\dfrac{K/k}{\mathfrak{p}^*}\right)$.

Théorème 5. Si $\bar{\sigma} = \text{corr.}_{\bar{K}} \sigma[\sigma \leqslant T_K(\mathfrak{P}^*)]$,

$$\beta_{-1}(\bar{\sigma}; \mathfrak{P}^*) = \beta_{-1}(\sigma; \mathfrak{P}^*)^{\nu-1}. \tag{7}$$

Démonstration. La contribution de $\mathfrak{P}$ dans $\bar{\mathfrak{P}}$ est $\mathfrak{P}^{\nu-1}$. Donc, si $\bar{\pi}$ est un entier de $\bar{K}$ d'ordre 1 en $\bar{\mathfrak{P}}$, $\dfrac{\bar{\pi}}{\pi^{\nu-1}} = \alpha \not\equiv 0 \pmod{\mathfrak{P}^*}$ et

$$\frac{\bar{\sigma}\bar{\pi}}{\bar{\pi}} = \frac{\sigma\bar{\pi}}{\bar{\pi}} = \frac{\sigma\alpha}{\alpha} \cdot \left(\frac{\sigma\pi}{\pi}\right)^{\nu-1} \equiv 1 \cdot \left(\frac{\sigma\pi}{\pi}\right)^{\nu-1} \pmod{\mathfrak{P}^*},$$

c'est-à-dire

$$\beta_{-1}(\bar{\sigma}; \mathfrak{P}^*) = \beta_{-1}(\sigma; \mathfrak{P}^*)^{\nu-1}. \qquad \text{C. Q. F. D.}$$

Ce théorème est le cas le plus simple d'un théorème général que je cite ici sans le démontrer, à cause de son importance et de l'élégance du résultat. La démonstration, qui sera donnée autre part, exige l'emploi des méthodes différentes de celles de ce travail $\sigma \leqslant T_K$ étant de niveau q ($q = 1, 0, 1, \ldots, m-1$),

désignons par $\beta(\sigma;\ \pi^*,\ \mathfrak{P}^*)$ la classe de restes (mod $\mathfrak{P}^*$) dans K^* à laquelle appartient $\frac{\sigma\pi-\pi}{\pi\pi^{*av_q}}$, c'est-à-dire $\beta(\sigma;\ \pi^*,\ \mathfrak{P}^*)=\beta_q(\sigma;\ \pi^*,\ \mathfrak{P}^*)$ quand $q\geqq 0$, et $=\beta_{-1}(\sigma;\ \mathfrak{P}^*)-1$ quand $q=-1$. *Alors a lieu l'égalité suivante : si* $\bar{\sigma}\leqslant T_{\bar{K}}$,

$$\beta(\bar{\sigma};\ \pi^*,\ \mathfrak{P}^*)=\prod_{\sigma\leqslant \text{gen.}_{T_K}\bar{\sigma}}\left(\beta(\sigma;\ \pi^*,\ \mathfrak{P}^*)\right). \tag{8}$$

Il est facile de vérifier que pour $\lambda_{\bar{K}/k}(\sigma;\ \mathfrak{P}^*)=-1$, cette égalité donne le théorème 5; quand $\lambda_{\bar{K}/k}(\bar{\sigma};\ \mathfrak{P}^*)\geqq -1$, elle peut se transcrire ainsi : soit σ un des éléments de $\text{gen.}_{T_K}\bar{\sigma}$ du plus grand niveau possible dans K/k. Si $\lambda_{\bar{K}/k}(\bar{\sigma})=q$, on a $\lambda_{K/k}(\sigma)=i_q$. Posons $\beta=\beta_{i_q}(\sigma;\ \pi^*,\ \mathfrak{P}^*)$. Désignons par $\mathfrak{M}_j$ l'ensemble $\beta_j^{(q)}(\nu;\ \pi^*,\ \mathfrak{P}^*)$ et par $\mathfrak{M}'_j$ le même ensemble sans élément 0. Alors

$$\beta_q(\bar{\sigma};\ \pi^*,\ \mathfrak{P}^*)=\Delta_0\prod_{\alpha\equiv\beta\ (\text{mod}\ \mathfrak{M}_{i_q})}(\alpha^{\nu_{i_q+1}})\cdot\prod_{j=0}^{i_q-1}\prod_{\alpha\leqslant\mathfrak{M}'_j}(\alpha^{\nu_{j+1}}) \tag{9}$$

(cette formule est encore vraie, si $\lambda_{\bar{K}/k}(\bar{\sigma})>q$. Dans ce cas $\beta\leqslant\mathfrak{M}_{i_q}$ et la formule donne $\beta_q(\bar{\sigma})=0$).

On peut écrire encore, si μ'_j désigne l'ensemble $M_j(K/\bar{K};\ \pi^*,\ \mathfrak{P}^*)$ sans l'élément 0,

$$\beta_q(\bar{\sigma};\ \pi^*,\ \mathfrak{P}^*)=\Delta_0\prod_{\alpha\equiv\beta\ (\text{mod}\ \mathfrak{M}_{i_q})}(\alpha^{\nu_{i_q+1}})\cdot\prod_{j=0}^{t'_q}\prod_{\alpha\leqslant\mu'_j}(\alpha^{\nu_{j+1}}) \tag{10}$$

où $t'_q=t_q-1$ ou t_q, suivant que $t_q=$ ou $\neq i_q$.

4° Cas particuliers du théorème 2 :

a. Si $K/\bar{K}$ *n'est pas ramifié par* rapport à $\mathfrak{P}$, on a $\nu_{-1}=\nu_0=\nu_1=\ldots=\nu_{m-1}=1$; donc

$$i_q=q\ (q=-1,0,1,\ldots,m),\quad \bar{v}_q=\sum_{s=0}^{q}\frac{v_s-v_{s-1}}{1}=v_q\quad\text{et}\quad \bar{n}_q=\frac{n_q}{\nu_q}=n_q.$$

b. Si l'ordre de $\mathfrak{P}$ *par rapport à* $\bar{K}$ *est premier à* p, c'est-à-dire $\nu_{-1}=\Delta_0$, on a $\nu_0=\nu_1\ldots=\nu_m=1$; on a encore $i_q=q$ $(q=-1,\ 0,\ 1,\ \ldots,\ m)$. Ici $\Delta_q=\frac{\nu_{-1}}{\nu_q}=\Delta_0$ $(q=0,\ 1,\ \ldots,\ m)$; donc

$$\bar{v}_q=\sum_{s=0}^{q}\frac{v_s-v_{s-1}}{\Delta_0}=\frac{1}{\Delta_0}\sum_{s=0}^{q}(v_s-v_{s-1})=\frac{v_q}{\Delta_0} \tag{11}$$

et $\bar{n}_q=\frac{n_q}{\nu_q}=\frac{n_q}{\Delta_0}$ ou n_q suivant, que $q=$ ou $\neq -1$.

c. Si $K/\overline{K}$ *est ramifiée d'ordre* p *par rapport à* $\mathfrak{P}$ *avec le nombre de ramification* $w = v_i$ *pour* $\mathfrak{P}$ on a : α) *si* $r_i > p$, $i_q = q$ et $\bar{v}_q = v_q$ ou $w + \dfrac{v_q - w}{p}$, suivant que $q \leqq i$ ou $\geqq i$. $n_q = \dfrac{n_q}{p}$ ou n_q, suivant que $q \geqq i$ ou $q > i$;

β) *si* $r_i = p$, $i_q = q$ pour $q < i$, et $i_q = q + 1$ pour $q \geqq i$; donc $\bar{v}_q = v_q$ ou $w + \dfrac{v_{q+1} - w}{p}$ et $\bar{n}_q = \dfrac{n_q}{p}$ ou n_{q+1}, suivant que $q < i$ ou $q \geqq i$.

B. — PROBLÈMES RÉCIPROQUES A CELUI DE LA PARTIE A

1° La partie A de ce chapitre fut consacrée à la détermination de certains objets définis dans un corps $\overline{K}$ (ensembles de décomposition, de ramification d'ordre q, nombres de ramification, fonction $i_k(\bar{\sigma})$, etc.) à partir d'objets correspondants d'un surcorps K de $\overline{K}$ et du corps rélatif $K/\overline{K}$. Ici nous nous occuperons des problèmes en quelque sorte réciproques de ceux de la partie A. Nous chercherons à déterminer certains objets dans le corps K/k à partir d'objets analogues dans son sous-corps $\overline{K}/k$ et dans le corps relatif $K/\overline{K}$. Il faut dire que cela n'est pas possible pour tous les objets dont on s'est occupé dans A : par exemple, les $\overset{(q)}{V}_K$ ne sont pas déterminés (même à automorphisme près) à partir des $\overset{(q)}{V}_{\overline{K}}$ et $\overset{(q)}{V}_{K/\overline{K}}$, du moins dans le cas général. Mais, par exemple, les v_q se déterminant à partir des $\bar{v}_q$, w_q, $n_q(K/\overline{K})$, on peut déterminer les $\overset{(q)}{V}_K$. $G_{K/\overline{K}}$, et l'on peut déterminer les $M_q(K/k;\ \pi^*,\ \mathfrak{P}^*)$ à partir des $M_q(\overline{K}/k;\ \pi^*,\ \mathfrak{P}^*)$ et des $M_q(K/\overline{K};\ \pi^*,\ \mathfrak{P}^*)$ (la solution de ce dernier problème sera exposée dans le travail consacré à la démonstration de la formule (8) de la partie A de ce chapitre).

2° Nous conservons les notations de A de ce chapitre. Cherchons à caractériser les t_q à partir des $\bar{v}_q$ et des w_q. Par définition, $w_{t_q} \leqq v_{i_q} < w_{t_q+1}$. Donc, puisque

$$\bar{v}_q = \frac{v_{i_q} - w_{t_q}}{\Delta'_{t_q+1}} + \sum_{j=0}^{t_q} \frac{w_j - w_{j-1}}{\Delta'_j},$$

on a

$$\bar{v}_q - \sum_{j=0}^{t_q} \frac{w_j - w_{j-1}}{\Delta'_j} \geqq 0 > \bar{v}_q - \sum_{j=0}^{t_q+1} \frac{w_j - w_{j-1}}{\Delta'_j} \tag{1}$$

et le signe d'égalité $0 = \bar{v}_q - \sum_{j=0}^{t_q} \dfrac{w_j - w_{j-1}}{\Delta'_j}$ n'a lieu que si $v_{i_q} = w_{t_q}$, c'est-à-dire $i_q = \varepsilon_{t_q}$.

L'égalité (1) définit les t_q à partir des objets définis dans $\overline{K}/k$ et $K/\overline{K}$.

Lemme 1. Tout $q = -1, 0, 1, \ldots, m$ est ou bien un des $\varepsilon_{-1}, \varepsilon_0, \ldots, \varepsilon_\mu$, ou bien un des $i_{-1}, i_0, \ldots, i_{\overline{m}}$ (il peut arriver que q fasse partie des deux ensembles à la fois).

Démonstration. Si q ne coïncide avec aucun des ε_s ($s = -1, 0, 1, \ldots\ldots, \mu$), on a $\rho_q = 1$; si q ne coïncide avec aucun des i_s ($s = -1, 0, 1, \ldots\ldots, \overline{m}$), on a $r_q = \rho_q$; donc, si le lemme n'était pas vrai pour un q, on aurait $r_q = 1$, ce qui est impossible. C. Q. F. D.

Désignons par $t_{e_1}, t_{e_2}, \ldots, t_{e_\lambda}$ tous les t_q (écrits dans l'ordre des grandeurs croissantes) tels que ε_{t_q} ne soit pas parmi les i_s ($s = -1, 0, 1, \ldots\ldots, \overline{m}$), c'est-à-dire tels que $\overline{v}_q \neq \sum_{j=0}^{t_q} \frac{w_j - w_{j-1}}{\Delta'_j}$.

Alors a lieu le

Théorème 1. $m = \mu + \lambda$; si $t_{e_s} + s < q < t_{e_{s+1}} + s + 1$, on a $v_q = w_{q-s}$; si $q = t_{e_s} + s$, on a

$$(2)\quad v_q = w_{t_{e_s}} + \Delta'_{t_{e_s}+1}\left(\overline{v}_{e_s} - \sum_{j=0}^{t_{e_s}} \frac{w_j - w_{j-1}}{\Delta'_j}\right) = w_{t_{e_s}} + \Delta'_{t_{e_s}+1}\overline{v}_{e_s} - \frac{1}{\nu'_{t_{e_s}+1}} \sum_{j=0}^{t_{e_s}} \nu'_j (w_j - w_{j-1}).$$

Si $e_s < q \leqq e_{s+1}$, on a

$$(3)\quad {}^{(t_{q-1}+s+1)}\mathrm{V}_K \cdot G_{K/\overline{K}} = {}^{(t_{q-1}+s+2)}\mathrm{V}_K \cdot G_{K/\overline{K}} = \ldots\ldots = {}^{(t_q+s)}\mathrm{V}_K \cdot G_{K/\overline{K}} = \mathrm{gen}._K\, {}^{(q)}\mathrm{V}_{\overline{K}},$$

si $q = e_{s+1}$, on a de plus ${}^{(t_q+s+1)}\mathrm{V}_K \cdot G_{K/\overline{K}} = \mathrm{gen}._K\, {}^{(q)}\mathrm{V}_{\overline{K}}$.

Démonstration. Par définition, il y a exactement s nombres de ramification de $\mathfrak{P}^*$ dans K/k qui ne sont pas parmi les w_q et qui sont $< w_{t_{e_s}+1}$, et parmi ceux-ci il y en a un qui est $> w_{t_{e_s}}$. Donc, il n'y en a aucun qui soit à la fois $\geqq w_{t_{e_s}+1}$ et $\leqq w_{t_{e_{s+1}}}$. Donc, si $t_{e_s} < q' \leqq t_{e_{s+1}}$, on a $w_{q'} = v_{q'+s}$, c'est-à-dire, en posant $q = q' + s$, $v_q = w_{q-s}$ quand $t_{e_s} + s < q < t_{e_{s+1}} + s + 1$. On a $i_{e_s} = t_{e_s} + s$. Donc, si $q = t_{e_s} + s$, on a

$$\overline{v}_{e_s} = \frac{v_q - w_{t_{e_s}}}{\Delta'_{t_{e_s}+1}} + \sum_{j=0}^{t_{e_s}} \frac{w_j - w_{j-1}}{\Delta'_j};$$

d'où

$$v_q = w_{t_{e_s}} + \Delta'_{t_{e_s}+1}\left(\bar{v}_{e_s} - \sum_{j=0}^{t_{e_s}} \frac{w_j - w_{j-1}}{\Delta'_j}\right) = w_{t_{e_s}} + \Delta'_{t_{e_s}+1}\bar{v}_{e_s} - \frac{1}{\nu'_{t_{e_s}+1}} \sum_{j=0}^{t_{e_s}} \nu'_j (w_j - w_{j-1})$$

si $e_s < q \leqq e_{s+1}$, $i_q = t_q + s$ ou $t_q + s + 1$, suivant que $q <$ ou $= e_{s+1}$. Donc, on a toujours $i_{q-1} = t_{q-1} + s$, et gen.$_K \overset{(q)}{V}_{\bar{K}} = \overset{(i)}{V}_K . G_{K/\bar{K}}$ pour $t_{q-1} + s + 1 \leqq i \leqq t_q + s$, et, si $q = e_{s+1}$, aussi pour $i = t_q + s + 1$. Le théorème est démontré.

Théorème **2.** Si $e_s < j \leqq e_{s+1}$, et si $t_{j-1} + s < q \leqq t_j + s$ ou $t_j + s + 1$, suivant que $j <$ ou $= e_{s+1}$, on a

$$n_q = \bar{n}_j \nu'_{q-s} \qquad \text{ou} \qquad \bar{n}_j \nu'_{q-s-1}$$

suivant que $q <$ ou $= t_{e_{s+1}} + s + 1$.

Démonstration. Si $t_{e_s} + s < q \leqq t_{e_{s+1}} + s = 1$, on a, suivant que $q <$ ou $= t_{e_{s+1}} + s + 1$, $\nu_q = \nu'_{q-s}$ ou ν'_{q-s-1}; si $e_s < j \leqq e_{s+1}$, $t_{e_s} + s < t_{j-1} + s + 1 \leqq t_j + s$ ou $t_j + s + 1 \leqq t_{e_{s+1}} + s + 1$, et, si $t_{j-1} + s < q \leqq t_j + s$ ou $t_j + s + 1$, suivant que $j <$ ou $= e_{s+1}$, cela signifie que $i_{j-1} + 1 \leqq q \leqq i_j$, c'est-à-dire corr.$_{\bar{K}} \overset{(q)}{V}_K = \overset{(j)}{V}_{\bar{K}}$; d'où le théorème.

3° *Autres réciproques des problèmes traités dans la partie* A. — On peut se poser encore le problème suivant, autre réciproque du problème traité dans la partie A de ce chapitre : Étant donnés les v_q, n_q, $M_q(K/k; \pi^*, \mathfrak{P}^*)$; $\bar{v}_q$, $\bar{n}_q$, $M_q(\bar{K}/k; \pi^*, \mathfrak{P}^*)$, déterminer les w_q, ν'_q, $M_q(K/\bar{K}); \pi^*, \mathfrak{P}^*)$. Mais ici ces nombres et ensembles ne peuvent pas être donnés arbitrairement, et, en fait, il s'agit dans ce problème plutôt de déterminer les conditions auxquelles doivent satisfaire les $v_q(\mathfrak{P}^*)$, $n_q(\mathfrak{P}^*)$, $M_q(\pi^*, \mathfrak{P}^*)$ dans K/k et dans $\bar{K}/k$ pour que le problème ne soit pas contradictoire.

Les formules et les problèmes de ce chapitre se trouvent en corrélation avec certaines formules et problèmes de la théorie locale des corps de classes : ainsi, par exemple, au théorème 2 de A correspond le *Führer-Discriminantensatz* de M. Hasse (2).

Dans cette corrélation le rôle de $G_{\bar{K}/k}$ joue, en quelque sorte, le groupe

(2) *Journ. f. d. reine und ang. Math.* 1930, t. 162, p. 169-184.

quotient du groupe de tous les nombres de k par le groupe de ceux qui sont normes des nombres de K (K étant supposé local et Abelien par rapport à k). J'ai pu trouver la formule sur le symbole $\left(\frac{\alpha, K}{\mathfrak{p}}\right)$ de M. Hasse qui correspond à la formule $\beta(\bar{\sigma}) = \prod_{\sigma \leqslant \text{gen.}_T \bar{\sigma}} \beta(\sigma)$; d'autre part, j'ai pu entrevoir, tout au moins en partie, certaines lois de dualité entre les $M_q(K/\overline{K})$ et les $M_q(\overline{K}/k)$ qui correspondent aux lois de dualité pour les corps Kummeriens que M. Hasse [3] a déduites de la loi de réciprocité pour le symbole de restes normiques $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$ de M. Hilbert $\left(\left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = \left(\frac{\beta, \alpha}{\mathfrak{p}}\right)^{-1}\right)$, et j'ai pu ainsi donner à ces dernières lois une forme explicite dans certains cas particuliers. Je parlerai de ces questions dans un travail futur.

Une question très curieuse est voisine de celle qui a été résolue dans cette partie B du chapitre III : celle de l'étude du caractère de la ramification d'un idéal d'un corps composé à partir des caractères de la ramification des idéaux correspondants dans les corps composants (cette question fut abordée par Herband dans la deuxième partie de son travail cité du *Journal des Mathématiques pures et appliquées,* **1931**; il a consacré à cette question encore quelques pages dans la première partie de son mémoire sur les *Corps algébriques de degré infini* (« deux lemmes sur les corps de degré fini ») [4]; malheureusement, les résultats qu'il y donne sont inexacts, du moins dans cette généralité, comme on peut le montrer par des contre-exemples simples [5]). Je consacrerai à la théorie des corps composés un travail spécial.

---

[3] « Neuere Untersuchungen in der Theorie alg. Zahlen ». Teil II : « Reziprozitätsgesetz ».

[4] *Math. Annalen*, 1932, t. 106, p. 473-501.

[5] L'inexactitude des résultats sur les corps composés que Herbrand donne dans son mémoire de *Math Annalen* a été remarquée aussi par un mathématicien japonais, M. Moriya, qui s'occupe des corps de degré infini. L'analyse des travaux de M. Moriya a été faite récemment par M. Hasse dans *Zentralblatt f. Math.*, 1936, t. 14, fasc. 6, p. 248.

CHAPITRE IV

PROPRIÉTÉS DES NOMBRES DE RAMIFICATION

1° Nous nous proposons d'étudier dans ce chapitre les propriétés des nombres de ramification d'un idéal dans un corps. Dans ce chapitre le corps à étudier (non-galoisien, en général) sera désigné par $\overline{K}/k$ et un de ses surcorps galoisiens sera désigné par K/k; $\mathfrak{P}$, $\overline{\mathfrak{P}}$, $\mathfrak{p}$ désigneront les idéaux correspondants de K, $\overline{K}$, k.

Quand $\overline{K}/k$ sera regardé comme un sous-corps de K/k, on se servira des mêmes notations qu'au chapitre III.

Le théorème que nous voulons démontrer, tout d'abord, est le

Théorème 1. Quand on met $v_q(\overline{\mathfrak{P}};\ \overline{K}/k)$ sous la forme d'une fraction irréductible, son dénominateur est premier à p,

Remarquons que dans la démonstration de ce théorème on peut, soit remplacer $\overline{K}/k$ par $\overline{K}(\overline{\mathfrak{P}})/k(\mathfrak{p})$, soit remplacer K par le corps de décomposition de $K/\overline{K}$ pour $\mathfrak{P}$ (sans changer k), parce que $\mathfrak{P}$ a (en vertu de resp. 1° de B de chapitre II et théorème 1 de B de chapitre III) dans ces corps les mêmes nombres de ramification que dans $\overline{K}/k$. Donc, on peut supposer qu'il existe un surcorps galoisien K/k de $\overline{K}/k$ où $\overline{\mathfrak{P}}$ n'a qu'un seul facteur premier $\mathfrak{P}$; donc, d'après le théorème 21 de A de chapitre II, on peut supposer existants les corps de ramification de tous ordres q, $-1 \leqq q \leqq m$, de $\overline{K}/k$ pour $\overline{\mathfrak{P}}$, soient

$$\overline{K}_{-1}, \overline{K}_0, \overline{K}_1, \ldots, \overline{K}_{\overline{m}-1}, \overline{K}_{\overline{m}} = \overline{K}. \tag{1}$$

Je désigne par $\overline{\mathfrak{P}}_{-1}$, $\overline{\mathfrak{P}}_0$, $\overline{\mathfrak{P}}_1$, ..., $\overline{\mathfrak{P}}_{\overline{m}-1}$, $\overline{\mathfrak{P}}_{\overline{m}}$ les idéaux premiers divisibles par $\overline{\mathfrak{P}}$ de ces corps respectifs.

Lemme 1. Les corps de ramification de $\overline{K}_{q+1}/k$ $(0 \leqq q < m)$ pour $\overline{\mathfrak{P}}_{q+1}$ sont $\overline{K}_{-1}$, $\overline{K}_0$, $\overline{K}_1$, ..., $\overline{K}_q$, $\overline{K}_{q+1}$. Les nombres de ramification finis de $\overline{\mathfrak{P}}_{q+1}$ dans

$\overline{K}_{q+1}/k$ coïncident avec les $q+1$ premiers nombres de ramification du $\mathfrak{P}$ dans K/k (c'est-à-dire $\bar{v}_{-1}, \bar{v}_0, v_1, \ldots, \bar{v}_q$).

Démonstration. Le corps $\overline{K}$ jouant le rôle de K de chapitre III et le corps K_{q+1} jouant le rôle de $\overline{K}$ de chapitre III, on a

$$\varepsilon_{-1} = -1, \varepsilon_0 = q+1, \varepsilon_1 = q+2, \ldots, \varepsilon_{m-q-1} = m; \; i_{-1} = -1, i_0 = 0, \ldots, i_q = q, i_{q+1} = m.$$

Il en résulte $t_0 = t_1 = \ldots \quad \ldots = t_q = -1$; d'où

$$v_0(\overline{\mathfrak{P}}_{q+1}; \overline{K}_{q+1}/\overline{k}) = \bar{v}_0 - 0 = \bar{v}_0, v_1(\overline{\mathfrak{P}}_{q+1}; \overline{K}_{q+1}/k) = \bar{v}_1, \ldots, v_q(\overline{\mathfrak{P}}_{q+1}; \overline{K}_{q+1}/k) = \bar{v}_q$$

et $v_{q+1}(\overline{\mathfrak{P}}_{q+1}; \overline{K}_{q+1}/k) = +\infty$; enfin, si $s \leqq q$, on a

$$\overset{(s)}{V}_{\overline{K}_{q+1}/k}(\mathfrak{P}) = \mathrm{corr}._{\overline{K}_{q+1}} \overset{(s)}{V}_{\overline{K}/k}(\mathfrak{P});$$

donc le corps de ramification d'ordre s de $\overline{K}_{q+1}/k$ pour $\overline{\mathfrak{P}}_{q+1}$ appartient à l'hypergroupe

$$\mathrm{gen}._{\overline{K}} \overset{(s)}{V}_{\overline{K}_{q+1}/k}(\mathfrak{P}) = \overset{(s)}{V}_{\overline{K}/k}(\mathfrak{P}) \cdot G_{\overline{K}/K_{q+1}} = \overset{(s)}{V}_{\overline{K}/k}(\mathfrak{P}) \cdot \overset{(q+1)}{V}_{\overline{K}/k}(\mathfrak{P}) = \overset{(s)}{V}_{\overline{K}/k}(\mathfrak{P}),$$

parce que $\overset{(q+1)}{V}_{\overline{K}/k}$ est un sous-hypergroupe de $\overset{(s)}{V}_{\overline{K}/k}$, c'est-à-dire le corps de ramification d'ordre s de $\overline{K}_{q+1}/k$ pour $\overline{\mathfrak{P}}_{q+1}$ est $\overline{K}_s$ ($s = -1, 0, 1, \ldots, q$); c'est encore vrai pour $s = q+1$ et le lemme est démontré.

Conséquence. $\overline{K}_{q+1}$ est le corps de ramification d'ordre 1 de $\overline{K}_{q+1}/\overline{K}_q$ pour $\overline{\mathfrak{P}}_{q+1}$ et $v_0(\overline{\mathfrak{P}}_{q+1}; \overline{K}_{q+1}/\overline{K}_q) = v_q$.

Première démonstration du théorème 1. Considérons la différente $\mathfrak{d}_{\overline{K}_{q+1}/\overline{K}_q}$ de $\overline{K}_{q+1}/\overline{K}_q$. La conséquence précédente et l'expression de la différente donnée à la fin de la partie A du chapitre II montrent que l'ordre de $\mathfrak{d}_{\overline{K}_{q+1}/\overline{K}_q}$ en $\overline{\mathfrak{P}}_{q+1}$ est $(\bar{r}_q - 1)(1 + \bar{v})$. Comme $\bar{r}_q$ est une puissance de p, $\bar{r}_q - 1$ est premier à p, et comme l'ordre en $\overline{\mathfrak{P}}_{q+1}$ de $\mathfrak{d}_{\overline{K}_{q+1}/\overline{K}_q}$ est entier, le dénominateur de $\bar{v}_q$ doit être premier à p.

Remarque. La démonstration précédente donne en même temps une nouvelle démonstration de ce que $\bar{r}_q - 1$ se divise par le dénominateur de $\bar{v}_q$.

Deuxième démonstration du théorème 1. Au 4° de la partie B de chapitre III nous avons démontré que si $\overline{K}/k$ est une extension locale égale à $\overline{K}_1/\overline{K}_0$ et

si $\bar{v}$ est son seul nombre de ramification propre, dont le dénominateur soit $\bar{\delta}$, tous les conjugués $\sigma\bar{\pi}$ d'un nombre $\bar{\pi}$ de $\overline{\mathrm{K}}$ d'ordre 1 en $\overline{\mathfrak{P}}$ se trouvent dans le corps obtenu par l'adjonction à k de $\sqrt[\bar{\delta}]{\bar{\pi}}$ et de toutes les racines de l'unité d'ordre premier à p qui se trouvent dans les classes (mod $\overline{\mathfrak{P}}$) appartenant à $\mathrm{M}_0(\overline{\mathrm{K}}/k\,;\ \sqrt[\bar{\delta}]{\bar{\pi}},\ \overline{\mathfrak{P}})$, où l'on suppose que K est choisi de manière à contenir $\sqrt[\bar{\delta}]{\bar{\pi}}$.

Il existe donc un développement normal de $\bar{\sigma}\bar{\pi}$, où $\bar{\sigma} \leqslant G_{\overline{\mathrm{K}}/k}$, suivant les puissances fractionnaires de $\bar{\pi}$, soit

$$\bar{\sigma}\bar{\pi} = \bar{\pi}(1 + \rho_1\bar{\pi}^{\bar{v}} + \rho_2\bar{\pi}^{\bar{u}_2} + \cdots + \rho_n\bar{\pi}^{\bar{u}_n} + \cdots), \tag{2}$$

où $u_1 = \bar{v} < u_2 < \ldots \quad \ldots < u_n < \ldots$ sont des fractions rationnelles dont les dénominateurs divisent $\bar{\delta}$, et où $\rho_1, \rho_2, \ldots, \rho_n, \ldots$ sont des racines de l'unité d'ordre premier à p appartenant à un corps circulaire de degré fini. Soit p^s la contribution de p dans $\bar{\delta}$ et supposons que $s > 0$. Soit K′ le surcorps circulaire de k qu'on obtient en adjoignant à k toutes les racines de l'unité indiquées, soit $\mathrm{K}'' = (\mathrm{K}', \overline{\mathrm{K}}) = \mathrm{K}'(\bar{\pi})$ et enfin soit $\mathrm{K}''' = \mathrm{K}'(\sqrt[\bar{\delta}]{\bar{\pi}})$. Il existe un isomorphisme σ''' de $\mathrm{K}'''/\mathrm{K}''$ qui transforme $\sqrt[\bar{\delta}]{\bar{\pi}}$ en $\varepsilon\sqrt[\bar{\delta}]{\bar{\pi}}$, où $\varepsilon^{\nu} = 1$, mais $\varepsilon \neq 1$. On a $\sigma'''\rho_n = \rho_n$ $(n = 1, 2, \ldots)$, parce que σ''' laisse invariants les nombres de K′. Comme σ''' laisse invariants les nombres de k, $\sigma'''(\bar{\sigma}\bar{\pi})$ est un conjugué par rapport à k de $\bar{\pi}$. Or, posant $\sqrt[\bar{\delta}]{\bar{\pi}} = \pi$, on a

$$\begin{aligned}\sigma'''(\bar{\sigma}\bar{\pi}) &= \sigma'''\bar{\pi}(1 + (\sigma'''\rho_1)(\sigma'''\pi)^{\bar{\delta}\bar{v}} + (\sigma'''\rho_2)(\sigma'''\pi)^{\bar{\delta}u_2} + \cdots + (\sigma'''\rho_n)(\sigma'''\pi)^{\bar{\delta}u_n} + \cdots)\\ &= \bar{\pi}(1 + \rho_1\varepsilon^{\bar{\delta}\bar{v}}\pi^{\bar{\delta}\bar{v}} + \rho_2\varepsilon^{\bar{\delta}u_2}\pi^{\bar{\delta}u_2} + \cdots + \rho_n\varepsilon^{\bar{\delta}u_n}\pi^{\bar{\delta}u_n} + \cdots)\end{aligned}$$

c'est-à-dire, si l'on pose

$$\mathrm{A} = \sum_{n=2}^{+\infty}(1 - \varepsilon^{\bar{\delta}u_n})\rho_n\pi^{\bar{\delta}u_n},$$

on a

$$\bar{\sigma}\bar{\pi} - \sigma'''(\bar{\sigma}\bar{\pi}) = [(1 - \varepsilon^{\bar{\delta}\bar{v}})\rho_1\pi^{\bar{\delta}\bar{v}} + \mathrm{A}]\bar{\pi}.$$

Or, $\bar{\delta}\bar{v}$ est premier à p; donc, si $\overline{\mathrm{E}}$ désigne l'ordre absolu de $\overline{\mathfrak{P}}$, l'ordre de $1 - \varepsilon^{\bar{\delta}\bar{v}}$ en $\overline{\mathfrak{P}}$ est $\dfrac{\overline{\mathrm{E}}}{p-1}$, et celui de $(1 - \varepsilon^{\bar{\delta}\bar{v}})\rho_1\pi^{\bar{\delta}\bar{v}}$ est $\dfrac{\overline{\mathrm{E}}}{p-1} + \bar{v}$, tandis que l'ordre en $\overline{\mathfrak{P}}$ de A est $\geqq$ que $\dfrac{\overline{\mathrm{E}}}{p-1} + u_2 > \dfrac{\overline{\mathrm{E}}}{p-1} + v$. Il en résulte

que : 1° $\bar{\sigma}\bar{\pi} \neq \sigma'''(\bar{\sigma}\bar{\pi})$; 2° $\bar{\sigma}\bar{\pi} \equiv \sigma'''(\bar{\sigma}\bar{\pi}) \pmod{\bar{\mathfrak{P}}\bar{\mathfrak{P}}^{a\bar{v}}}$, c'est-à-dire, si $\sigma'''(\bar{\sigma}\bar{\pi}) = \bar{\sigma}_1\bar{\pi}$, $\bar{\sigma}_1 \neq \bar{\sigma}$ et $\beta_0(\bar{\sigma}_1; \pi, \mathfrak{P}) = \beta_0(\bar{\sigma}; \pi, \mathfrak{P})$. Donc $\bar{\sigma}_1 < \bar{\sigma}$ $\overset{(1)}{\mathrm{V}}_{\bar{\mathrm{K}}/k} = \bar{\sigma}$. $\{1_{\bar{\mathrm{K}}}\} = \{\bar{\sigma}\}$ et l'on a, contrairement à 1°, que $\bar{\sigma}_1 = \bar{\sigma}$. Donc $s > 0$ est impossible et $\bar{\delta}$ est premier à p. Nous avons démontré du même coup que tous les u_n ont les dénominateurs premiers à p.

On n'a maintenant qu'à prendre $\overline{\mathrm{K}}_{q+1}(\overline{\mathfrak{P}}_{q+1})/\overline{\mathrm{K}}_q(\overline{\mathfrak{P}}_q)$ et lui appliquer le résultat précédent pour avoir le théorème 1.

2° *Dénominateurs des* $\bar{v}_q$.

Lemme 2. Soient K/k un corps galoisien, $t \leqslant \mathrm{T}_{\mathrm{K}/k}(\mathfrak{P})$, $\sigma \leqslant \overset{(q)}{\mathrm{V}}_{\mathrm{K}/k}(\mathfrak{P})$ $(q = 0, 1, 2, \ldots, m-1)$.

Alors $t\sigma t^{-1} \leqslant \overset{(q)}{\mathrm{V}}_{\mathrm{K}/k}(\mathfrak{P})$ et l'on a, π étant un nombre de K d'ordre 1 en $\mathfrak{P}$,

$$\beta_q(t\sigma t^{-1}; \pi, \mathfrak{P}) = \beta_{-1}(t; \mathfrak{P})^{v_q} \cdot \beta_q(\sigma; \pi, \mathfrak{P}). \tag{3}$$

Démonstration. On a $t\sigma t^{-1}\pi - \pi = t(\sigma t^{-1}\pi - t^{-1}\pi)$, et comme $t^{-1}\pi$ est d'ordre 1 en $\mathfrak{P}$ et $t\mathfrak{P} = \mathfrak{P}$, l'ordre en $\mathfrak{P}$ de $t\sigma t^{-1}\pi - \pi$ doit être égal à $1 + v_q$; d'où $t\sigma t^{-1} \leqslant \overset{(q)}{\mathrm{V}}$.

On tire de l'égalité précédente

$$\frac{t\sigma t^{-1}\pi - \pi}{\pi^{1+v_q}} = t\left[\frac{\sigma \cdot t^{-1}\pi - t^{-1}\pi}{(t^{-1}\pi)^{1+v_q}}\right] = \left(\frac{t\pi}{\pi}\right)^{v_q} \cdot t\left[\frac{\sigma \cdot t^{-1}\pi - t^{-1}\pi}{t^{-1}\pi \cdot \pi^{v_q}}\right]. \tag{4}$$

D'où

$$\beta_q(t\sigma t^{-1}; \pi, \mathfrak{P}) = \beta_{-1}(t; \mathfrak{P})^{v_q} \cdot \beta_q(\sigma; \pi, \mathfrak{P}). \qquad \text{C. Q. F. D.}$$

Conséquence. $\overset{(q)}{\mathrm{V}}_{\mathrm{K}/k}(\mathfrak{P})$ est un sous-groupe invariant de $\mathrm{T}_{\mathrm{K}/k}(\mathfrak{P})$. Si $t \leqslant \mathrm{V}_{\mathrm{K}/k}(\mathfrak{P})$, $t\sigma t^{-1} \equiv \sigma \pmod{\overset{(q+1)}{\mathrm{V}}_{\mathrm{K}/k}(\mathfrak{P})}$. La première partie est évidente; la deuxième suit de ce que si $t \leqslant \mathrm{V}$, on a $\beta_{-1}(t) = 1$; donc $\beta_q(t\sigma t^{-1}) = 1^{v_q}$. $\beta_q(\sigma) = \beta_q(\sigma)$.

Désignons $r_{-1}(\mathrm{K}/k; \mathfrak{P})$ par h. Alors a lieu le

Lemme 3. $v_q(r_q - 1) \equiv 0 \pmod{h}$.

Démonstration. L'ensemble de tous les $\beta_{-1}(t)$, $t \leqslant \mathrm{T}$, est l'ensemble de racines h-ièmes de l'unité dans $\mathfrak{R}$. Donc, si $h_q = \dfrac{h}{(h, v_q)}$, l'ensemble des $\beta_{-1}(t)^{v_q}$,

$t \leqslant T$, est l'ensemble de toutes les racines h_q-ièmes de l'unité dans $\mathfrak{R}$. De la définition de h_q il résulte que $h_q v_q \equiv 0 \pmod{h}$.

Subdivisons M_q en classes, deux éléments de M_q étant dans la même classe si leur quotient est une racine h_q-ième de l'unité. Puisque, quel que soit ζ tel que $\zeta^{h_q} = 1$, il existe un t de manière que $\beta_{-1}(t)^{v_q} = \zeta$, si $M \geqslant \beta = \beta_q(\sigma)$, aussi $M \geqslant \beta_q(t\,\sigma\,t^{-1}) = \zeta\beta$. Donc, dans chacune des classes ainsi définies il y a juste h_q éléments, à l'exception de la classe contenant 0, qui n'a qu'un élément. Par conséquent, $r_q - 1 \equiv 0 \pmod{h_q}$ et $(r_q - 1)v_q \equiv 0 \pmod{h}$. C. Q. F. D.

Théorème 2. Le dénominateur de $\bar{v}_q$ est

$$\frac{\rho_{-1}}{(\rho_{-1}, v_{i_q})} \tag{5}$$

et

$$\Delta_{i_q}\bar{v}_q \equiv v_{i_q} \pmod{\rho_{-1}}.$$

Démonstration. On a

$$\bar{v}_q = \frac{v_{i_q} - w_{t_q}}{\Delta'_{t_q+1}} + \sum_{s=0}^{t_q}\frac{w_s - w_{s-1}}{\Delta'_s} = \frac{v_{i_q}}{\Delta_{i_q}} + \sum_{s=1}^{t_q} w_s\left(\frac{1}{\Delta'_s} - \frac{1}{\Delta'_{s+1}}\right) = \frac{v_{i_q}}{\Delta_{i_q}} + \sum_{s=1}^{t_q}\frac{\Delta'_0}{\Delta'_{s+1}}\cdot\frac{w_s(\rho'_s - 1)}{\Delta'_0}.$$

En appliquant le lemme 3 au corps $K/\overline{K}$ on voit que $w_s(\rho'_s - 1) \equiv 0 \pmod{\Delta'_0 = \rho_{-1}}$. D'autre part, $\frac{\Delta'_{s+1}}{\Delta'_s}$ est une puissance de p. Donc, le dénominateur de $\sum_{s=1}^{t_q}\frac{\Delta'_0}{\Delta'_{s+1}}\cdot\frac{w_s(\rho'_s - 1)}{\Delta'_0}$ est une puissance de p. Le dénominateur de $\frac{v_{i_q}}{\Delta'_{s+1}} = \frac{v_{i_q}}{\rho_{-1}}\cdot\frac{\Delta'_0}{\Delta'_{s+1}}$ divise certainement $\frac{\rho_{-1}}{(v_{i_q}, \rho_{-1})}\cdot\frac{\Delta'_{s+1}}{\Delta_0}$ et est divisible par $\frac{\rho_{-1}}{(v_{i_q}, \rho_{-1})}$, donc est un produit de $\frac{\rho_{-1}}{(\rho_{-1}, v_{i_q})}$ par une puissance de p. Donc, le dénominateur de $\bar{v}$ est aussi un produit de $\frac{\rho_{-1}}{(\rho_{-1}, v_{i_q})}$ par une puissance de p; et comme, d'après le théorème 1, il est premier à p, il doit être $\frac{\rho_{-1}}{(\rho_{-1}, v_{i_q})}$. Comme $\Delta_{i_q}\sum_{s=1}^{t_q} w_s\left(\frac{1}{\Delta'_s} - \frac{1}{\Delta_{s+1}}\right) \equiv 0 \pmod{\rho_{-1}}$, on a $\Delta_{i_q}\bar{v}_q \equiv v_{i_q} \pmod{\rho_{-1}}$. C. Q. F. D.

Conséquence. Si maintenant $K \geqq \overline{K} > \overline{\overline{K}} > k$, $\overline{i_q} = i_q(\mathfrak{P}; \overline{K}, \overline{\overline{K}}, k)$,

$\overline{\rho}_{-1} = r_{-1}(\overline{\mathrm{K}}/\overline{\overline{\mathrm{K}}}; \mathfrak{P})$, on a évidemment, $\overline{\delta_q}$, $\overline{\overline{\delta}}_q$ désignant les dénominateurs des $\overline{v}_q = v_q(\overline{\mathrm{K}}/k; \mathfrak{P})$ et $\overline{\overline{v}}_q = v_q(\overline{\overline{\mathrm{K}}}/k; \mathfrak{P})$, que

$$\overline{\delta}_{i_q} \mid \overline{\overline{\delta}}_q \mid \overline{\delta}_{i_q}\overline{\rho}_{-1}. \tag{6}$$

En particulier, si $\overline{\rho}_{-1} = 1$, on a $\overline{\delta}_{i_q} = \overline{\overline{\delta}}_q$.

Démonstration. En effet, $r_{-1}(\mathrm{K}/\overline{\overline{\mathrm{K}}}; \mathfrak{P}) = r_{-1}(\mathrm{K}/\overline{\mathrm{K}}; \mathfrak{P}) \cdot \overline{\rho}_{-1}$. Donc

$$\frac{r_{-1}(\mathrm{K}/\overline{\mathrm{K}}; \mathfrak{P})}{\left(v_{i_{\overline{i}_q}}, r_{-1}(\mathrm{K}/\overline{\mathrm{K}}; \mathfrak{P})\right)} \text{ divise } \frac{r_{-1}(\mathrm{K}/\overline{\overline{\mathrm{K}}}; \mathfrak{P})}{\left(v_{i_{\overline{i}_q}}, r_{-1}(\mathrm{K}/\overline{\overline{\mathrm{K}}}; \mathfrak{P})\right)}, \text{ qui divise } \frac{r_{-1}(\mathrm{K}/\overline{\mathrm{K}}; \mathfrak{P}) \cdot \overline{\rho}_{-1}}{\left(v_{i_{\overline{i}_q}}, r_{-1}(\mathrm{K}/\overline{\mathrm{K}}; \mathfrak{P})\right)}.$$

Or, il est bien évident que $i_q(\mathfrak{P}; \mathrm{K}, \overline{\overline{\mathrm{K}}}, k) = i_{\overline{i}_q}(\mathfrak{P}; \mathrm{K}, \overline{\mathrm{K}}, k)$; d'où la proposition.

3° Intégrité des nombres de ramification. — Nous allons démontrer maintenant une proposition très curieuse qui donne la condition pour que *tous* les $\overline{v}_q$ soient entiers. La partie directe de ce théorème (le caractère suffisant de la condition indiquée) nous donnera une troisième démonstration du théorème 1, indépendante de deux précédentes. Dans la démonstration de la réciproque seront démontrées, en passant, des propositions sur les corps galoisiens ayant de l'intérêt par elles-mêmes. Donc, il s'agit de démontrer

Théorème 3. La condition nécessaire et suffisante pour que tous les $\overline{v}_q$ $(q = 1, 0, 1, \ldots, \overline{m} - 1)$ soient entiers est que $\tau = \mathrm{T}_{\mathrm{K}/\overline{\mathrm{K}}}(\mathfrak{P})$ fasse partie de l'une des suites de composition de $\mathrm{T} = \mathrm{T}_{\mathrm{K}/k}(\mathfrak{P})$.

Remarque. Dans la démonstration de ce théorème on peut supposer $G_{\mathrm{K}/\overline{\mathrm{K}}} = \tau$ et $G_{\mathrm{K}/k} = \mathrm{T}$. En effet, le corps d'inertie K_τ de $\mathrm{K}/\overline{\mathrm{K}}$ pour $\mathfrak{P}$ a les mêmes nombres de ramification par rapport à k que le corps $\overline{\mathrm{K}}$, parce que $n_{-1}(\mathrm{K}_\tau/\overline{\mathrm{K}}; \mathfrak{P}) = 1$. Il est évident que ces nombres de ramification restent encore les mêmes si on les prend par rappport au corps d'inertie K_T de K/k pour $\mathfrak{P}$. D'autre part, $G_{\mathrm{K}/\mathrm{K}_\tau} = \mathrm{T}_{\mathrm{K}/\mathrm{K}_\tau} = \tau$ et $G_{\mathrm{K}/\mathrm{K}_\mathrm{T}} = \mathrm{T}_{\mathrm{K}/\mathrm{K}_\mathrm{T}} = \mathrm{T}$.

Lemme 4. $\overline{\mathrm{K}}/k$ étant tel que $\overline{\mathrm{K}}_q$ et $\overline{\mathrm{K}}_{q+1}$ existent, s'il existe un corps $\overline{\overline{\mathrm{K}}}$, $\overline{\mathrm{K}}_q < \overline{\overline{\mathrm{K}}} \leqq \overline{\mathrm{K}}_{q+1}$ tel que $\overline{\overline{\mathrm{K}}}/\overline{\mathrm{K}}_q$ soit Galoisien, $\overline{v}_q$ est entier.

Démonstration. On a vu que $\overline{\mathrm{K}}_q$ et $\overline{\mathrm{K}}_{q+1}$ sont des corps de ramification d'ordre respectif 0,1 de $\overline{\mathrm{K}}_{q+1}/\overline{\mathrm{K}}_q$ pour $\mathfrak{P}_{q+1}$ et que $v_0(\overline{\mathrm{K}}_{q+1}/\overline{\mathrm{K}}_q;\mathfrak{P}) = \bar{v}_q$. Or, il suit du théorème 2 de la partie A du chapitre II qu'il en est de même pour $\overline{\overline{\mathrm{K}}}/\overline{\mathrm{K}}_q$ et que $v_0(\overline{\overline{\mathrm{K}}}/\overline{\mathrm{K}}_q;\mathfrak{P}) = v_0(\overline{\mathrm{K}}_{q+1}/\overline{\mathrm{K}}_q;\mathfrak{P}) = \bar{v}_q$. Puisque $\overline{\mathrm{K}}/\overline{\mathrm{K}}_q$ est Galoisien, $\bar{v}_q = v_0(\overline{\overline{\mathrm{K}}}/\overline{\mathrm{K}}_q;\mathfrak{P})$ est entier. C. Q. F. D.

Démonstration de la proposition directe : si τ fait partie d'une suite de composition de T, *tous les* $\bar{v}_q$ $(q = -1, 0, 1, \ldots, \overline{m}-1)$ *sont entiers.* Soit $\mathrm{T} = \Phi_0, \Phi_1, \ldots\ldots, \Phi_s = \tau, \Phi_{s+1}, \ldots\ldots, \{1_{\mathrm{K}}\}$ une suite de composition de T dont τ fasse partie. Soit q un des nombres $0, 1, \ldots, \overline{m}-1$; soit $\Psi_i = \Phi_i \overset{(i_{q+1})}{\mathrm{V}}_{\mathrm{K}}$ $(i = 0, 1, \ldots\ldots, s, s+1, \ldots)$. Les Ψ_i sont des groupes, parce que $\overset{(i_{q+1})}{\mathrm{V}}_{\mathrm{K}}$ est un sous-groupe invariant de T. De plus, Ψ_{i+1} est invariant dans Ψ_i. On a $\Psi_0 = \mathrm{T} \geqq \overset{(i_q)}{\mathrm{V}}_{\mathrm{K}}\tau = \mathrm{gen.}_{\mathrm{K}} \overset{(q)}{\mathrm{V}}_{\mathrm{K}}$ et $\Psi_s = \overset{(i_{q+1})}{\mathrm{V}}_{\mathrm{K}} \cdot \tau = \mathrm{gen.}_{\mathrm{K}} \overset{(q+1)}{\mathrm{V}}_{\overline{\mathrm{K}}}$. Donc, il existe un j, $0 < j \leqq s$, tel que $\Psi_{j-1} \geqq \mathrm{gen.}_{\mathrm{K}} \overset{(q)}{\mathrm{V}}_{\overline{\mathrm{K}}}$, tandis que $\Psi_j < \mathrm{gen.}_{\mathrm{K}} \overset{(q)}{\mathrm{V}}_{\overline{\mathrm{K}}}$. D'ailleurs, puisque quand $\Psi_{i-1} \neq \Psi_i$, on a $\Psi_{i-1}/\Psi_i \simeq \Phi_{i-1}/\Phi_i$, c'est-à-dire Ψ_{i-1}/Ψ_i est simple, on doit avoir (puisque $\Psi_{j-1} \neq \Psi_j$) $\Psi_{j-1} = \mathrm{gen.}_{\mathrm{K}} \overset{(q)}{\mathrm{V}}_{\overline{\mathrm{K}}}$. Donc à Ψ_{j-1} appartient le corps $\overline{\mathrm{K}}_q$, et le corps $\overline{\overline{\mathrm{K}}}$ qui appartient à Ψ_j est son surcorps Galoisien.

Comme évidemment, $\overline{\overline{\mathrm{K}}} \leqq \overline{\mathrm{K}}_{q+1}$, les conditions du lemme 4 sont satisfaites et $\bar{v}_q$ est entier. C. Q. F. D.

Nous allons maintenant employer un important théorème de Sylow sur les p — groupes.

Théorème de Sylow. Le normalisateur d'un vrai sous-groupe γ d'un p — groupe G est un vrai (c'est-à-dire $\neq \gamma$) surgroupe de γ.

Démonstration. c étant un élément de G, appelons *catégorie de* c (suivant γ) [1] l'ensemble $\gamma c \gamma$.

Il est facile de voir que deux catégories, ou bien coïncident, ou bien sont disjointes, et que le nombre de classes suivant γ contenues dans $\gamma c \gamma$ est égal à l'indice de $\gamma \wedge c\gamma c^{-1}$ dans γ. Puisque γ est un p — groupe, cet

(1) Ce nom est de M. F. Marty (*Annales de l'École norm. sup.* 1936).

indice est une puissance positive ou nulle (ce qui arrive si, et seulement si $c\gamma c^{-1} = \gamma$, c'est-à-dire c appartient au normalisateur $N(\gamma)$ de γ) de p. Soit $G = \gamma c_1 \gamma + \gamma c_2 \gamma + \dots \quad \dots + \gamma c_n \gamma$ une décomposition de G en somme de catégories disjointes. Soit λ_i le nombre de classes suivant γ que contient $\gamma c_i \gamma$; alors

$$(G : \gamma) = \lambda_1 + \lambda_2 + \dots + \lambda_n .$$

Si γ est un vrai sous-groupe de G, c'est-à-dire $G \neq \gamma$, $(G : \gamma)$ se divise par p. Si le normalisateur $N(\gamma)$ de γ était γ, parmi les λ_i il n'y en aurait qu'un seul égal à 1, et les autres seraient divisibles par p. On arriverait à la conclusion absurde $0 \equiv 1 \pmod{p}$, ce qui démontre le théorème

Conséquence 1. Tout sous-groupe γ d'un p — groupe G fait partie d'une suite de composition de G. G est résoluble (²).

En effet, si l'on pose $N_i(\gamma) = N[N_{i-1}(\gamma)]$, il existe i tel que $N_i(\gamma) = G$, car autrement, puisque, quand $N_i(\gamma) \neq G$, $N_{i+1}(\gamma)$ est un vrai surgroupe de $N_i(\gamma)$, il y aurait dans G des sous-groupes d'ordre aussi grand que l'on veut. Donc, si $G = N_i(\gamma) \neq N_{i-1}(\gamma)$, $N_i(\gamma)$, $N_{i-1}(\gamma)$, ..., $N_1(\gamma)$. γ, $\{I\}$, est une suite normale de G, qu'on peut toujours compléter jusqu'à avoir une suite de composition; ce qui démontre la première affirmation. Soit $G = \gamma_0, \gamma_1, \dots, \gamma_n = \{I\}$ une suite de composition de G. γ_i/γ_{i+1} $(i = 0, 1, \dots, u-1)$ est un p — groupe simple; donc, d'après ce qui précède, il ne peut avoir de vrai sous-groupe. Il en résulte que son ordre est p, et G est résoluble.

Conséquence 2. T est résoluble; le degré du corps $\overline{\overline{K}}$, introduit précédemment, par rapport à K_q est p.

En effet, $T/V = (T/V)^{(T)}$ est Abelien, d'après chapitre II, A, et V est un p — groupe, donc résoluble, d'où T est résoluble. Comme $\Psi_{j+1}/\Psi_j \simeq \Phi_{j-1}/\Phi_j$, on a $(\overline{\overline{K}} : \overline{K_q}) = (\Psi_{j-1} : \Psi_j) = (\Phi_{j-1} : \Phi_j) = p$. C. Q. F. D.

Troisième démonstration du théorème 1. Considérons le corps de ramification K_ν de $K/\overline{K}$ pour $\mathfrak{P}$, appartenant à $\nu = V_{K/\overline{K}}(\mathfrak{P})$, $K_\nu/\overline{K}$ est ramifié d'ordre ρ_{-1} premier à p pour $\mathfrak{P}$. D'après le chapitre III, A, les nombres de ramifica-

(²) Cette dernière partie de cette conséquence est connue sous le nom de la « deuxième loi de Sylow ».

tion de $\overline{K}/k$ se déduisent de ceux de K_ν/k en les divisant par ρ_{-1}. On a $T_{K/k} = T$ et $T_{K/K_\nu} = \nu$. La conséquence du théorème du Sylow montre que ν fait partie d'une suite de composition de $V = V_{K/k}$ et aussi, puisque V est sous-groupe invariant de T (lemme 4), d'une suite de composition de T. Il en résulte que les nombres de ramification de K_ν/k sont entiers et que ceux de $\overline{K}/k$ ont les dénominateurs premiers à p. C. Q. F. D.

Maintenant nous nous occuperons de la démonstration de la réciproque :

Soit t un élément de T d'ordre $h(t)$ premier à p. Alors $\beta_{-1}(t)$ est une racine primitive $h(t)$ -ième de l'unité dans $\mathfrak{R}$. Il résulte de ce qui précède le

Lemme 5. Pour que les commutateurs de $t \leqslant T$ d'ordre $h(t)$ premier à p par des éléments de $\overset{(q)}{V}_K (q \geq 0)$ soient dans $\overset{(q+1)}{V}_K$, il est nécessaire et suffisant que

$$v_q \equiv 0 \pmod{h(t)}; \tag{7}$$

si $v_q \not\equiv 0 \pmod{h(t)}$, les éléments de $\overset{(q+1)}{V}_K$ sont les seuls éléments de $\overset{(q)}{V}_K$ dont les commutateurs par t sont dans $\overset{(q+1)}{V}_K$.

Démonstration. Si $\sigma \leqslant V_K$, la condition nécessaire et suffisante pour que le commutateur de t par σ soit dans $\overset{(q+1)}{V}_K$ est que $\beta_q(t\sigma t^{-1}) = \beta_q(\sigma)$. Or $\beta_q(t\sigma t^{-1}) = \beta_{-1}(t)^{v_q} \cdot \beta_q(\sigma)$. Donc, si $\beta_q(\sigma) \neq 0$, c'est-à-dire si σ n'est pas dans $\overset{(q+1)}{V}_K$, la condition écrite équivaut à $\beta_{-1}(t)^{v_q} = 1$, c'est-à-dire à $v_q \equiv 0 \pmod{h(t)}$, ce qui démontre le lemme.

Théorème 4. Si $t \leqslant T$ est d'ordre $h(t)$ premier à p et si $v_q \equiv 0 \pmod{h(t)}$, il existe dans chaque classe de $\overset{(q)}{V}_K(\mathfrak{P})$ suivant $\overset{(q+1)}{V}_K(\mathfrak{P})$ un élément permutable avec t; si $v_q \not\equiv 0 \pmod{h(t)}$, il n'en existe que dans la classe égale à $\overset{(q+1)}{V}_K(\mathfrak{P})$ lui-même.

Démonstration. Supposons que $v_q \equiv 0 \pmod{h(t)}$. Soit $\sigma \leqslant \overset{(q)}{V}_K$. l étant $> q$; nous allons montrer par récurrence sur l qu'il existe dans $\overset{(q)}{V}$ un élément σ_l tel que $\sigma_l \equiv \sigma \pmod{\overset{(q+1)}{V}}$ et que $t\sigma_l t^{-1}\sigma_l^{-1} \leqslant \overset{(l)}{V}$. D'après le lemme 5, la proposition est vraie pour $l = q + 1$.

Posons $t\sigma_l t^{-1} = \tau_l \sigma_l$, $\tau_l \leqslant \overset{(l)}{\mathrm{V}}$, et distinguons deux cas :

1° Si $v_l \equiv 0 \pmod{h(t)}$, on a $\beta_l(t\tau_l t^{-1}) = \beta_l(\tau_l)$, c'est-à-dire $t\tau_l t^{-1} \equiv \tau_l \pmod{\overset{(l+1)}{\mathrm{V}}}$. D'où, pour a quelconque,

$$t^a \sigma_l t^{-a} \equiv \tau_l^a \sigma_l \pmod{\overset{(l+1)}{\mathrm{V}}}. \tag{8}$$

En faisant $a = h(t)$, il vient $\sigma_l = \tau_l^{h(t)} \sigma_l \pmod{\overset{(l+1)}{\mathrm{V}}}$; d'où $\tau_l^{h(t)} \equiv 1 \pmod{\overset{(l+1)}{\mathrm{V}}}$. Puisque $h(t)$ est premier à p et que l'ordre de $\overset{(l)}{\mathrm{V}} / \overset{(l+1)}{\mathrm{V}}$ est une puissance de p, on a $\tau_l \leqslant \overset{(l+1)}{\mathrm{V}}$, et l'on peut poser $\sigma_{l+1} = \sigma_l$.

2° Soit $v_l \not\equiv 0 \pmod{h(t)}$. D'après le lemme 2, $\mathrm{M}_l(\mathrm{K}/k;\ \pi,\ \mathfrak{P})$ est un module par rapport au corps fini engendré par ζ^{v_l}, où ζ est une racine primitive h-ième de l'unité dans $\mathfrak{R}$, et, à fortiori, puisque $h(t) \mid h$, par rapport au corps fini engendré par $\beta_{-1}(t)^{v_l}$. On a $\beta_{-1}(t)^{v_l} - 1 \neq 0$, et l'on pourra trouver $\tau_l' \leqslant \overset{(l)}{\mathrm{V}}$ tel que

$$\beta_l(\tau_l') = \frac{-1}{\beta_{-1}(t)^{v_l} - 1} \beta_l(\tau_l); \tag{9}$$

d'où

$$\beta_l(t\tau_l' t^{-1} \tau_l'^{-1}) = \beta_l(t\tau_l' t^{-1}) + \beta_l(\tau_l'^{-1}) = (\beta_{-1}(t)^{v_l} - 1)\,\beta_l(\tau_l') = -\beta_l(\tau_l),$$

c'est-à-dire

$$t\tau_l' t^{-1} \tau_l'^{-1} \equiv -\tau_l \pmod{\overset{(l+1)}{\mathrm{V}}};$$

en posant

$$\sigma_{l+1} = \sigma_l \tau'$$

on a

$$t\sigma_{l+1} t^{-1} \sigma_{l+1}^{-1} = t\sigma_l \tau_l' t^{-1} \tau_l'^{-1} \sigma_l^{-1} = t\sigma_l t^{-1} \cdot t\tau_l' t^{-1} \tau_l'^{-1} \cdot \sigma_l^{-1} \equiv \tau_l \sigma_l \tau_l^{-1} \sigma_l^{-1} \equiv 1_{\mathrm{K}} \pmod{\overset{(l+1)}{\mathrm{V}}},$$

c'est-à-dire $\leqslant \overset{(l+1)}{\mathrm{V}}$, ce qui achève la démonstration de la première partie du théorème, car σ_m est bien permutable avec t et $\equiv \sigma \pmod{\overset{(l+1)}{\mathrm{V}}}$.

Si $v_q \not\equiv 0 \pmod{h(t)}$, le commutateur de t par tout $\sigma \leqslant \overset{(q)}{\mathrm{V}}$ qui n'est pas dans $\overset{(q+1)}{\mathrm{V}}$ n'appartient pas à $\overset{(q+1)}{\mathrm{V}}$, donc à fortiori n'est pas égal à 1_{K}. Donc un tel élément ne peut pas être permutable avec t. C. Q. F. D.

Démonstration de la deuxième partie du théorème 3. *Si tous les* $\bar{v}_q$ ($q = -1, 0, 1, \ldots, \bar{m} - 1$ *sont entiers,* τ *fait partie d'une suite de composition*

de T. Il existe dans τ un élément t d'ordre ρ_{-1} (pour l'avoir, il suffit, par exemple, d'élever dans une puissance de p convenable n'importe quel élément de la classe de τ suivant ν qui engendre τ/ν). Désignons par $w(t)$ le groupe de tous les éléments de V_K permutables avec t. Remarquons que si q n'est pas parmi les nombres $i_{-1}, i_0, i_1, \ldots, i_{\bar{m}-1}$, $\overset{(q+1)}{\nu V_K} \geqq \overset{(q)}{V_K}$, parce que dans chaque classe de $\overset{(q)}{V_K}$ suivant $\overset{(q+1)}{V_K}$ il y des éléments de $\nu = V_{K/\bar{K}}$. De même, si $v_q \equiv 0 \pmod{\rho_{-1}}$, $w(t).\overset{(q+1)}{V_K} \geqq \overset{(q)}{V_K}$, parce que, d'après le théorème 4, il y a alors dans chaque classe de $\overset{(q)}{V_K}$ suivant $\overset{(q+1)}{V_K}$ des éléments de $w(t)$.

D'après le théorème 2, le dénominateur de $\bar{v}_q$ est $\frac{\rho_{-1}}{(v_{i_q}, \rho_{-1})}$. Donc, si tous les $\bar{v}_q$ sont entiers, $v_{i_q} \equiv 0 \pmod{\rho_{-1}}$ pour tout q; donc, si $v_q \not\equiv 0 \pmod{\rho_{-1}}$, q n'est pas parmi les nombres $i_{-1}, i_0, i_1, \ldots, i_{\bar{m}-1}$.

Posons $W = w(t).\nu$. Montrons que $W\overset{(q+1)}{V_K} \geqq \overset{(q)}{V_K}$. En effet, ou bien $v_q \equiv 0 \pmod{\rho_{-1}}$, et alors $W\overset{(q+1)}{V_K} \geqq w(t)\overset{(q+1)}{V_K} \geqq \overset{(q)}{V_K}$; ou bien q n'est pas parmi les nombres $i_{-1}, i_0, i_1, \ldots, i_{\bar{m}-1}$, et alors $W\overset{(q+1)}{V_K} \geqq \nu\overset{(q+1)}{V_K} \geqq \overset{(q)}{V_K}$. Il s'ensuit que si $\overset{(q+1)}{V_K} \leqq W$, aussi $\overset{(q)}{V_K} \leqq W$. Donc, puisque $\overset{(m)}{V_K} = \{1_K\} \leqq W$, on a $W = V_K$.

Par suite, si Φ est un groupe tel que $V_K \geqq \Phi \geqq \nu$, on a $t\Phi t^{-1} = \Phi$. D'après la conséquence du théorème de Sylow, V_K étant un p-groupe, il existe une suite de composition de V_K qui passe par ν. Soient $V_K = \Phi_0, \Phi_1, \ldots, \Phi_s = \nu$ les premiers termes de cette suite.

Soit Θ le groupe engendré par t et posons $U_i = \Theta\Phi_i$. Puisque $t\Phi_i t^{-1} = \Phi_i$, on a $\Theta\Phi_i = \Phi_i\Theta$, et U_i est un groupe dont Φ_i est un sous-groupe invariant. Comme $U_{i+1} \wedge \Phi_i = \Phi_{i+1}$ est un sous-groupe invariant de Φ_i, U_{i+1} est un sous-groupe invariant de U_i et $(U_i : U_{i+1}) = (\Phi_i : \Phi_{i+1}) = p$. U_0 est un sous-groupe invariant de $T = T_K$ et T/U_0 est cyclique d'ordre $\frac{r_{-1}}{\rho_{-1}} = \bar{r}_{-1}$; $U_s = \theta\nu = \theta V_{K/\bar{K}} = T_{K/\bar{K}} = \tau$. Il en résulte qu'il existe une suite de composition de T qui passe par τ. C. Q. F. D.

4° Les ω-corps de ramification. — Théorème 4 nous servira à introduire pour le cas des extensions galoisiennes K/k certains sous-groupes caractéristiques de $V_{K/k}$ (1) autres que ceux de Hilbert et les surcorps caractéristiques de K_0 qui leur appartiennent.

Définition 1. Un corps $K^{(\omega)}$, ω étant un diviseur de $h = r_{-1}(K/k; \mathfrak{P})$, tel que $K \geq K^{(\omega)} \geq K_0$, s'appelle un *$\omega$-corps de ramification* de K/k pour $\mathfrak{P}$, s'il satisfait aux conditions suivantes : *a*) tous les nombres de ramification de $\mathfrak{P}$ dans $K/K^{(\omega)}$ sont divisibles par ω; *b*) aucun des nombres de ramification propres de $\mathfrak{P}$ dans $K^{(\omega)}/k$ n'est divisible par ω; *c*) il existe un corps $\overline{K}^{(\omega)}$, $K^{(\omega)} > \overline{K}^{(\omega)} \geq k$, tel que $(K^{(\omega)} : \overline{K}^{(\omega)}) = \omega$ et que $K^{(\omega)}/\overline{K}^{(\omega)}$ soit complètement ramifié pour $\mathfrak{P}$.

[Il serait d'ailleurs à rechercher si la condition *c*) n'est pas une conséquence des *a*) et *b*)].

Théorème 6. Si l'on pose $\overline{K} = K^{(\omega)}$, on a, avec les notations de chapitre III, $\rho_q = r_q$, si $v_q \equiv 0 \pmod{\omega}$ et $\rho_q = 1$, si $v_q \not\equiv 0 \pmod{\omega}$.

Démonstration. Il est évident que $\rho_q = 1$ si $v_q \not\equiv 0 \pmod{\omega}$, car autrement $\mathfrak{P}$ aurait dans $K/\overline{K} = K/K^{(\omega)}$ un nombre de ramification non divisible par ω; supposons que pour un q tel que $v_q \equiv 0 \pmod{\omega}$ on ait $\rho_q \neq r_q$; alors q est un nombre i_s. Dans $\overline{K}/k = K^{(\omega)}/k$ $\mathfrak{P}$ a un nombre de ramification $\bar{v}_s = \sum_{j=0}^{q} \frac{v_j - v_{j-1}}{\Delta_j}$ engendré par v_q. Par suite $\mathfrak{P}$ a dans $\overline{K}^{(\omega)}/k$ un nombre de ramification, engendré par v_q, qui est $\frac{\bar{v}_s}{\omega}$. Le dénominateur de ce nombre est $\frac{\omega}{(v_q, \omega)} = \frac{\omega}{\omega} = 1$. Donc $\bar{v}_s \equiv 0 \pmod{\omega}$ contre l'hypothèse *b*), et $\rho_q \neq r_q$ est impossible. C. Q. F. D.

Théorème 7. Si $t \leqslant T_{K/k}$ est d'ordre ω, et si $w(t)$ est le groupe de tous les éléments de $V_{K/k}$ permutables avec t, le corps qui appartient à $w(t)$ dans K est un ω-corps de ramification de K/k pour $\mathfrak{P}$; inversement, tout ω-corps de ramification de K/k pour $\mathfrak{P}$ appartient dans K au groupe $w(t)$ défini par un $t \leqslant T_{K/k}$ d'ordre ω.

Démonstration. 1° Désignons par $\overline{K}$ le corps qui appartient à $w(t)$. Il est évident, d'après le théorème 4, que $\rho_q = r_q$ ou 1, suivant que $v_q \equiv$ ou $\not\equiv 0 \pmod{\omega}$. Puisque $\rho_q \equiv 1$ quand $v_q \not\equiv 0 \pmod{\omega}$, la condition *a*) est satisfaite. θ étant le groupe engendré par t, puisque $t \cdot w(t) \cdot t^{-1} = w(t)$, $\theta \cdot w(t)$ est un groupe et le corps $\overline{\overline{K}}$ qui lui appartient est tel que $\overline{K}/\overline{\overline{K}}$ satisfait à la condition *c*). Enfin, si $q \geq 0$, $v_{i_q} \not\equiv 0 \pmod{\omega}$. On a

$$\bar{v}_q = \sum_{s=0}^{i_q} \frac{v_s - v_{s-1}}{\Delta_s} \qquad \text{et} \qquad v_q(\mathfrak{P}; \overline{\overline{K}}/k) = \frac{\bar{v}_q}{\omega}$$

et $i_q(\mathfrak{P}; K, \overline{\overline{K}}, k) = i_q(\mathfrak{P}; K, \overline{K}, k) = i_q$; donc le dénominateur de $\frac{\bar{v}_q}{\omega}$ est $\frac{\omega}{(\omega, v_{i_q})} > 1$ et $\bar{v}_q \not\equiv 0 \pmod{\omega}$. La condition b) est vérifiée et $\overline{K}$ est un $K^{(\omega)}$.

2° Soit $K^{(\omega)}$ un ω-corps de ramification. Dans le groupe de $K/\overline{K}^{(\omega)}$ (qui fait partie de $T_{K/k}$), il y a un élément t d'ordre ω. Supposons $G_{K/K^{(\omega)}} \neq w(t)$. Alors, il existe un j tel que $G_{K/K^{(\omega)}} \wedge \overset{(j+1)}{V}_{K/k} \leq w(t)$ et que $G_{K/K^{(\omega)}} \wedge \overset{(j)}{V}_{K/k}$ ne soit pas contenu dans $w(t)$. Soit σ un élément de $G_{K/K'^{(\omega)}} \wedge \overset{(j)}{V}_{K/k}$ qui n'est pas dans $w(t)$. D'après le théorème 7, $v_j \equiv 0 \pmod{\omega}$; donc $t\sigma t^{-1}\sigma^{-1} \leqslant \overset{(j+1)}{V}_{K/k}$. Comme cet élément est encore dans $V_{K/\overline{K}^{(\omega)}} = G_{K/K^{(\omega)}}$, on a $t\sigma t^{-1} = \sigma\sigma_1$, où $\sigma_1 \leqslant w(t)$; mais alors $t^2\sigma t^{-2} = t\sigma t^{-1} \cdot t\sigma_1 t^{-1} = \sigma\sigma_1 \cdot \sigma_1 = \sigma\sigma_1^2$, et, en général, $t^a\sigma t^{-a} = \sigma\sigma_1^a$; en particulier, $\sigma = t^\omega \sigma t^{-\omega} = \sigma\sigma_1^\omega$, c'est-à-dire $\sigma_1 = 1_K$, contre l'hypothèse que σ n'est pas dans $w(t)$. Donc $G_{K/K^{(\omega)}} = w(t)$, et le théorème est démontré.

Théorème 8. Tous les ω-corps de ramification de K/k pour $\mathfrak{P}$ sont conjugués entre eux par rapport à K_0.

Démonstration. Puisque dans deux sous-groupes cycliques de $T_{K/k}$, θ et θ', du même ordre ω premier à p, on peut choisir des éléments t et t' d'ordre ω tels que $t \equiv t' \pmod{V_{K/k}}$, il suffit de montrer qu'il existe pour de tels t, t' un $\sigma \leqslant V_{K/k}$ tel que $t' = \sigma t \sigma^{-1}$.

Montrons, par réccurence, que quel que soit $q \geq 0$, il existe un σ_q tel que $\sigma_q t \sigma_q^{-1} = t'\sigma_q'$ avec $\sigma_q' \leqslant \overset{(q)}{V}_{K/k}$. Pour $q = 0$ la proposition est vraie. Supposons-la vraie pour q. Distinguons deux cas :

1° $v_q \not\equiv 0 \pmod{\omega}$. Alors, si $\xi \leqslant \overset{(q)}{V}_{K/k}$, on a

$$\xi\sigma_q t\sigma_q^{-1}\xi^{-1} = t' \cdot t'^{-1}\xi t'\xi^{-1} \cdot \xi\sigma_q'\xi^{-1} \equiv t' \cdot t'^{-1}\xi t'\xi^{-1} \cdot \sigma_q' \pmod{\overset{(q+1)}{V}_{K/k}}.$$

On a vu dans la démonstration du théorème 5 qu'on peut trouver ξ de manière que $t'^{-1}\xi t'\xi^{-1} \equiv \sigma_q'^{-1} \pmod{\overset{(q+1)}{V}_{K/k}}$ et, si l'on pose $\sigma_{q+1} = \xi\sigma_q$, on a bien $\sigma_{q+1} t \sigma_{q+1}^{-1} t^{-1} \leqslant \overset{(q+1)}{V}_{K/k}$;

2° $v_q \equiv 0 \pmod{\omega}$; on a $t'\sigma_q' \equiv \sigma_q' t' \pmod{\overset{(q+1)}{V}_{K/k}}$, d'où $1_K \equiv \sigma_q t^\omega \sigma_q^{-1} \equiv t'^\omega \sigma_q'^\omega \equiv \sigma_q'^\omega \pmod{\overset{(q+1)}{V}_{K/k}}$; donc $\sigma_q' \leqslant \overset{(q+1)}{V}_{K/k}$ et l'on peut poser $\sigma_{q+1} = \sigma_q$.

$\sigma = \sigma_m$ satisfait à $t\sigma t^{-1} = t'$ et existe. Théorème est démontré.

5° Inégalités et égalités pour les nombres de ramification. — Nous voulons généraliser aux corps non-galoisiens deux théorèmes démontrés pour le cas

galoisien par M. Öystein Ore (3). Nous nous basons ici sur un théorème de M. Andreas Speiser (4), qui servit aussi de base à M. Ore. La démonstration simple que nous en donnons est due à M. Öystein Ore (5).

Théorème de Speiser. Si K/k est galoisien, le plus grand nombre de ramification propre v_{m-1} de $\mathfrak{P}$ dans K/k est $\leqq \frac{E}{p-1}$, où E est l'ordre absolu de $\mathfrak{P}$; si $v_{m-1} \equiv 0 \pmod p$, ce nombre est $\frac{E}{p-1}$.

Démonstration. Dans la démonstration de ce théorème on peut supposer K/k cyclique, parce qu'on peut remplacer k par le corps appartenant dans K à un sous-groupe d'ordre p de $\overset{(m-1)}{V}_{K/k}$. Ceci posé, $\mathfrak{d}_{K/k}$ a l'ordre $(p-1)+(p-1)v_0$ en $\mathfrak{P}$ (car $m=1$).

D'autre part, si

$$f(x) = x^p + a_1 x^{p-1} + \cdots + a_p = 0 \tag{10}$$

est l'équation irréductible à laquelle satisfait dans k un entier π de K d'ordre 1 en $\mathfrak{P}$, la contribution de $\mathfrak{P}$ dans $f'(\pi)$ est égale à celle de $\mathfrak{P}$ dans $\mathfrak{d}_{K/k}$.

Mais $f'(\pi) = p\pi^{p-1} + (p-1)a_1\pi^{p-2} + (p-2)a_2\pi^{p-3} + \ldots + a_{p-1}$. Tous les a_i ont les ordres en $\mathfrak{P}$ divisibles par p; donc tous les termes $(p-i)a_i\pi^{p-i}$ de $f'(\pi)$ ont des ordres en $\mathfrak{P}$ incongrus deux à deux (mod. p); donc, à fortiori, inégaux. Il en résulte que l'ordre en $\mathfrak{P}$ de $f'(\pi)$ est le minimum de ces ordres, donc, en particulier, ne dépasse pas celui de $p\pi^{p-1}$, égal à $(p-1)+E$; d'où $(p-1)v_0 \leqq E$ et $v_0 \leqq \frac{E}{p-1}$. Si $v_0 \equiv 0$ (mod. p), l'ordre en $\mathfrak{P}$ de $\mathfrak{d}_{K/k}$ est $\equiv p-1 \pmod p$; donc il doit être égal à l'ordre de $p\pi^{p-1}$, égal à $p-1+E$, et l'on a $v_0 = \frac{E}{p-1}$. C. Q. F. D.

Je me servirai encore d'un résultat dû à M. Ore : *si le corps galoisien* K/k *a un nombre de ramification propre divisible par* p, K($\mathfrak{P}$) *contient les racines primitives* p *-ièmes de l'unité* (3).

Théorème 9 (*Inégalité d'Ore*). $\overline{K}/k$ étant un corps algébrique, $\overline{E}$ étant l'ordre absolu de $\overline{\mathfrak{P}}$,

$$v_q(\overline{K}/k; \overline{\mathfrak{P}}) \cdot n_q(\overline{K}/k; \overline{\mathfrak{P}}) \leqq \overline{E}\,\frac{p}{p-1} \quad (q = -1, 0, 1, \ldots, \overline{m}-1). \tag{11}$$

---

(3) *Mathematische Annalen,* t. 102, 1929-30, p. 283-304.

(4) « Zerlegungsgruppe », *Journ. f. d. reine und ang. Math.*, 1919, t. 149 p. 174-188.

(5) *Mathematische Annalen,* t. 100, 1928, p. 650-683.

Démonstration. Tout d'abord, il suffit de démontrer ce théorème, reprenant la notation de 1°, 2°, 3° de ce chapitre, sous l'hypothèse $G_{K/\overline{K}} = V_{K/\overline{K}} = \nu$, parce que si l'on pose $K_\nu = K'$ et si l'on désigne par E', v'_q, n'_q resp. l'ordre absolu de l'idéal premier $\mathfrak{P}'$ de K' que divise $\mathfrak{P}$, $v_q(K'/k; \mathfrak{P}')$, $n_q(K'/k; \mathfrak{P}')$, on a $E' = \overline{E}\rho_{-1}$, $n'_q = \bar{n}_q$ et $v'_q = \bar{v}_q\rho_{-1}$, et le théorème est vrai dans $\overline{K}/k$ s'il est vrai dans K'/k. Cela posé, pour $q = -1$ le théorème est évident. Soit donc $q \geqq 0$. On a vu que, dans l'hypothèse $K_\nu = \overline{K}$, il existe $\overline{\overline{K}}$, $\overline{K}_{q+1} \geqq \overline{\overline{K}} > \overline{K}_q$, tel que $\overline{\overline{K}}/\overline{K}_q$ soit cyclique de degré p; $\overline{\overline{K}}/\overline{K}_q$ est complètement ramifié pour $\mathfrak{P}$, son nombre de ramification propre est $\bar{v}_q$ et l'ordre absolu de l'idéal premier $\overline{\mathfrak{P}}$ de $\overline{\overline{K}}$ que divise $\mathfrak{P}$ est évidemment $\frac{\overline{E}}{\bar{n}_q}p$. En appliquant le théorème de Speiser, on trouve $\bar{v}_q \leqq \frac{\overline{E}}{\bar{n}_q}\frac{p}{p-1}$; d'où $\bar{v}_q\bar{n}_q \leqq \frac{\overline{E}}{p-1}$. C. Q. F. D.

Théorème 10 (*Égalité d'Ore*). Si $\bar{v}_q \equiv 0 \pmod p$ on a 1) $\bar{v}_q\bar{n}_q = \frac{\overline{E}}{p-1}$; 2) $\bar{r}_q = p$. 3). Le corps de Galois $K^*(\mathfrak{P}^*)$ du $\overline{K}(\overline{\mathfrak{P}})$ par rapport à $k(\mathfrak{p})$ contient les racines p-ièmes primitives de l'unité ($0 \leqq q < m$).

Démonstration. On se place dans les mêmes conditions que pour le théorème précédent.

En appliquant la deuxième partie du théorème de Speiser à $\overline{\overline{K}}/\overline{K}_q$ on trouve $\bar{v}_q\bar{n}_q = \frac{\overline{E}}{p-1}$.

D'autre part, si l'on avait $\bar{r}_q = \frac{\bar{n}_q}{\bar{n}_{q+1}} > p$, il y aurait entre $\overline{K}_{q+1}$ et $\overline{\overline{K}}$ un corps $\overline{\overline{K}}'$ tel que $\overline{\overline{K}}'/\overline{\overline{K}}$ soit cyclique de degré p. Le seul nombre de ramification propre de $\mathfrak{P}$ dans $\overline{\overline{K}}'/\overline{\overline{K}}$ étant $\bar{v}_q$, on aurait, d'après la deuxième partie du théorème de Speiser,

$$\bar{n}_q\bar{v}_q = \overline{E}\frac{p^2}{p-1}, \tag{12}$$

ce qui est impossible; en appliquant le théorème d'Ore (évidemment vrai pour le cas local) au corps $\overline{K}(\overline{\mathfrak{P}})/k(\mathfrak{p})$, on voit que si $v_q \equiv 0 \pmod p$, le sous-corps du corps Galois $K^0(\mathfrak{P}^0)$ de $\overline{K}(\overline{\mathfrak{P}})$ par rapport à $k(\mathfrak{p})$ qui appartient à $V_{K^0(\mathfrak{P}^0)/K(\mathfrak{P})}$, donc aussi $K^0(\mathfrak{P}^0)$ lui-même, contient toutes les racines p-ièmes de l'unité. C. Q. F. D.

Autre expression du théorème 9 *et de* 1) *du théorème* 10. Soit e_0 l'ordre absolu de $\mathfrak{p}$ et soit $d_q(\overline{\mathrm{K}}/k;\ \overline{\mathfrak{P}}) = \frac{n_{q-1}(\overline{\mathrm{K}}/k;\ \overline{\mathfrak{P}})}{n_q(\overline{\mathrm{K}}/k;\ \overline{\mathfrak{P}})}$. On a $\frac{\overline{\mathrm{E}}}{n_q} = e_0 d_q(\mathrm{K}/k;\ \mathfrak{P})$. D'où l'on a comme expression du théorème 9 et de 1) du théorème 10 resp. $v_q(\overline{\mathrm{K}}/k;\ \overline{\mathfrak{P}}) \leqq e_0 d_q(\overline{\mathrm{K}}/k;\ \overline{\mathfrak{P}})\frac{p}{p-1}$ et $v_q(\overline{\mathrm{K}}/k;\ \overline{\mathfrak{P}}) = e_0 d_q(\overline{\mathrm{K}}/k;\ \overline{\mathfrak{P}})\frac{p}{p-1}$.

6° Congruences et inégalités pour les nombres de ramification d'un corps, correspondant a l'existence des sous-corps. — A partir d'ici les notations employées seront celles des chapitres précédents : le corps, en général non-galoisien, à étudier sera désigné par K/k (et non par $\overline{\mathrm{K}}/k$) et $\overline{\mathrm{K}}/k$ désignera un de ses sous-corps, aussi non-galoisien en général. Les théorèmes précédents permettent de déduire un certain nombre de congruences et d'inégalités qui lient les nombres de ramification de $\mathfrak{P}$ dans K/k, si l'on connaît l'existence d'un sous-corps $\overline{\mathrm{K}}/k$ de K/k caractérisé par les ν_q donnés.

Congruences suivant les puissances de p.

Théorème 11. $a_0, a_1, \ldots, a_{\overline{m}-1}$ étant des fractions rationnelles (pouvant être nulles) à dénominateur premier à p, si a lieu la congruence

$$\sum_{q=0}^{\overline{m}-1} a_q(\overline{v}_q - \overline{v}_{q-1}) \equiv 0 \pmod{p^\lambda}, \tag{13}$$

on a

$$\sum_{q=0}^{\overline{m}-1}\ \sum_{j=i_{q-1}+1}^{i_q} a_q \nu_j (v_j - v_{j-1}) \equiv \pmod{\nu_0 p^\lambda}. \tag{14}$$

En particulier, si $v_q \equiv \overline{v}_{q-1} \pmod{p^\lambda}$, on a

$$\sum_{j=i_{q-1}+1}^{i_q} \frac{\Delta_{i_q}}{\Delta_j}(v_j - v_{j-1}) \equiv 0 \left(\mod \frac{\nu_0}{\nu_{i_q}} p^\lambda\right);$$

on a

$$\sum_{j=i_{q-1}+1}^{i_q} \frac{\Delta_{i_q}}{\Delta_j}(v_j - v_{j-1}) \equiv 0 \left(\mod \frac{\nu_0}{\nu_{i_q}}\right). \tag{15}$$

Enfin, si pour tout $q = 0, 1, \ldots, m-1$ on a $\rho_q < r_q$ et si $\overline{v}_q \equiv \overline{v}_{q-1} \pmod{p^\lambda}$, on a $v_q \equiv v_{q-1} \left(\mod \frac{\nu_0}{\nu_q} p^\lambda\right)$; on a, si seulement la première condition est réalisée (c'est-à-dire $\lambda = 0$),

$$\overline{v}_q \equiv \overline{v}_{q-1} \left(\mod \frac{\nu_0}{\nu_q} = \rho_0 \rho_1 \ldots \rho_{q-1}\right). \tag{16}$$

Démonstration. On a

$$\bar{v}_q - \bar{v}_{q-1} = \sum_{j=0}^{i_q} \frac{v_j - v_{s-1}}{\Delta_j} - \sum_{j=0}^{i_{q-1}} \frac{v_j - v_{j-1}}{\Delta_j} = \sum_{j=i_{q-1}+1}^{i_q} \frac{v_j - v_{j-1}}{\Delta_j};$$

d'où

$$\sum_{q=0}^{\bar{m}-1} a_q (\bar{v}_q - \bar{v}_{q-1}) = \sum_{q=0}^{\bar{m}-1} \left(\sum_{j=i_{q-1}+1}^{i_q} a_q \frac{v_j - v_{j-1}}{\Delta_j} \right) = \sum_{q=0}^{\bar{m}-1} \sum_{j=i_{q-1}+1}^{i_q} \frac{a_q \nu_j}{\Delta_0 \nu_0} (v_j - v_{j-1})$$

$$= \frac{1}{\Delta_0 \nu_0} \sum_{q=0}^{\bar{m}-1} \sum_{j=i_{q-1}+1}^{i_q} a_j \nu_j (v_j - v_{j-1});$$

si cette expression est congrue 0 (mod p^λ),

$$\sum_{q=0}^{\bar{m}-1} \sum_{j=i_{q-1}+1}^{i_q} a_q \nu_j (v_j - v_{j-1}) \equiv 0 \pmod{\nu_0 p^\lambda}. \qquad \text{C. Q. F. D.}$$

En particulier, si $a_0 = a_q = \ldots \quad \ldots = a_{q-1} = a_{q+1} = \ldots \quad \ldots a_{\bar{m}-1} = 0$, $a_q = 1$, on a

$$\sum_{j=i_{q-1}+1}^{i_q} \frac{\Delta_{i_q}}{\Delta_j} (v_j - v_{j-1}) = \sum_{j=i_{q-1}+1}^{i_q} \frac{\nu_j}{\nu_{i_q}} (v_j - v_{j-1}) \equiv 0 \left(\mathrm{mod} \frac{\nu_0}{\nu_{i_q}} p^\lambda \right).$$

Et, en particulier, si $\rho_q < r_q$ pour tout $q \equiv 0, 1, \ldots \ldots, \bar{m} - 1$, c'est-à-dire $i_q = i_{q-1} + 1 = q$, on a

$$\sum_{j=i_{q-1}+1}^{q} \frac{\nu_j}{\nu_{i_q}} (v_j - v_{j-1}) = v_q - v_{q-1} \equiv 0 \left(\mathrm{mod} \frac{\nu_0}{\nu_q} p^\lambda \right).$$

Puisque la congruence initiale $\bar{v}_q \equiv \bar{v}_{q-1} \pmod{p^\lambda}$ est toujours vraie (d'après le théorème 1 de ce chapitre) pour $\lambda = 0$, les deux congruences précédentes sont toujours vraies pour $\lambda = 0$. Le théorème est démontré.

Congruences suivant ρ_{-1}. On a vu que pour tout $q = 0, 1, \ldots \quad \ldots, \bar{m} - 1$,

$$v_{i_q} \equiv \Delta_{i_q} \bar{v}_q \pmod{\rho_{-1}}. \tag{17}$$

Il en résulte que si un polynôme à coefficients entiers en $\Delta_{i_q} \bar{v}_q$ ($q = 0, 1, \ldots \quad \ldots, m - 1$) est $\equiv 0$ (mod. ρ_{-1}), ce polynôme prend encore une valeur $\equiv 0 \pmod{\rho_{-1}}$ quand on y remplace chaque $\Delta_{i_q} \bar{v}_q$ par v_{i_q} correspondant.

Autres congruences. Il est à remarquer que si tous les $v_q\,(q = 0, 1, \ldots \ldots, m-1)$ propres sont divisibles par un nombre u premier à ρ_{-1} et à p, tous les $\bar{v}_q\,(q = 0, 1, \ldots \ldots, \overline{m}-1)$ propres le sont aussi. L'inverse a lieu si pour tout $q = 0, 1, \ldots \ldots, m-1$ on a $\rho_q < r_q$: alors, de la divisibilité par u de tous les $\bar{v}_q$ propres suit celle de tous les v_q propres.

Inégalités. Nous poserons $\varphi_q = v_q n_q$. Désignons par E l'ordre absolu de $\mathfrak{P}$.

Théorème 12.

$$\varphi_{i_q} + \sum_{j=0}^{i_q-1} \varphi_j \frac{\rho_j - 1}{r_j} \prod_{s=j+1}^{i_q-1} \frac{\rho_s}{r_s} \leqq \mathrm{E}\,\frac{p}{p-1} \tag{18}$$

et, en particulier,

$$\sum_{j=i_{q-1}+1}^{i_q} \varphi_j \leqq \mathrm{E}\left(\frac{p}{p-1}\right)^2. \tag{19}$$

Démonstration. On a

$$\bar{v}_q = \frac{v_{i_q}}{\Delta_{i_q}} + \sum_{j=0}^{i_q-1} \frac{v_j(\rho_j - 1)}{\Delta_{j+1}} = \frac{v_{i_q}}{\Delta_{i_q}} + \sum_{j=0}^{i_q-1} \frac{v_j}{\Delta_j} \frac{\rho_j - 1}{\rho_j};$$

d'où

$$\bar{\varphi}_q = \bar{n}_q \bar{v}_q = \frac{n_{i_q}}{\nu_{i_q}} \bar{v}_q = \frac{n_{i_q} v_{i_q}}{\nu_{i_q} \Delta_{i_q}} + \sum_{j=0}^{i_q-1} \frac{n_j v_j}{\Delta_j \nu_j} \cdot \frac{\nu_j}{n_j} \frac{n_{i_q}}{\nu_{i_q}} \frac{\rho_j - 1}{\rho_j}$$

$$= \frac{1}{\nu_{-1}} \left(\varphi_{i_q} + \sum_{j=0}^{i_q-1} \varphi_j \frac{\rho_j - 1}{r_j} \cdot \frac{\nu_{j+1}}{\nu_{i_q}} \frac{n_{i_q}}{n_{j+1}} \right) = \frac{1}{\nu_{-1}} \left(\varphi_{i_q} + \sum_{j=0}^{i_q-1} \varphi_j \frac{\rho_j - 1}{r_j} \prod_{s=j+1}^{i_q-1} \frac{\rho_s}{r_s} \right).$$

Or, si $\overline{\mathrm{E}}$ est l'ordre absolu de $\overline{\mathfrak{P}}$, on a $\overline{\mathrm{E}} = \dfrac{\mathrm{E}}{\nu_{-1}}$, et, d'après le théorème 9, $\bar{\varphi}_q \leqq \overline{\mathrm{E}} \dfrac{p}{p-1} = \dfrac{\mathrm{E}}{\nu_{-1}} \dfrac{p}{p-1}$; d'où

$$\varphi_{i_q} + \sum_{j=0}^{i_q-1} \varphi_j \frac{\rho_j - 1}{r_j} \prod_{s=j+1}^{i_q-1} \frac{\rho_s}{r_s} \leqq \mathrm{E}\,\frac{p}{p-1}.$$

Mais, si $i_{q-1} < j < i_q$ et si $j \leqq s < i_q$, on a $i_{q-1} \cdot \ s < i_q$ et $\rho_s = r_s$; donc

$$\prod_{s=j+1}^{i_q-1} \frac{\rho_s}{r_s} = 1 \quad \text{et} \quad \frac{\rho_j - 1}{r_j} = \frac{r_j - 1}{r_j} = 1 - \frac{1}{r_j} \geqq 1 - \frac{1}{p}.$$

D'où

$$\varphi_{i_q} + \sum_{j=i_{q-1}+1}^{i_q-1} \varphi_j \frac{p_j - 1}{r_j} \prod_{s=j+1}^{i_q-1} \frac{\rho_s}{r_s} = \varphi_{i_q} + \sum_{j=i_{q-1}+1}^{i_q-1} \varphi_j \left(1 - \frac{1}{r_j}\right) \geqq \left(1 - \frac{1}{p}\right) \sum_{j=i_{q-1}+1}^{i_q} \varphi_j$$

et

$$\sum_{j=i_{q-1}+1}^{i_q} \varphi_j \leqq \frac{\mathrm{E}\,\dfrac{p}{p-1}}{1 - \dfrac{1}{p}} = \mathrm{E}\left(\frac{p}{p-1}\right)^2. \qquad \text{C. Q. F. D.}$$

7° Rang de $V^{(Z^*)}$.

Définition 2. Un ensemble $\{ c_1, c_2, \ldots \ \ldots, c_n \}$ d'éléments d'un hypergroupe $\mathfrak{H}$ s'appelle une *base* de $\mathfrak{H}$, si $\mathfrak{H}$ est le moindre hypergroupe qui le contient. Le minimum du nombre d'éléments n que peut avoir une base de $\mathfrak{H}$ s'appelle *rang de* $\mathfrak{H}$ et se désigne par $\mathfrak{R}(\mathfrak{H})$. Une base de $\mathfrak{H}$ dont le nombre d'éléments est $\mathfrak{R}(\mathfrak{H})$ s'appelle *une base de* $\mathfrak{H}$ *de rang minimum* (à remarquer que pour les groupes Abeliens notre définition du rang coïncide avec la définition habituelle).

Les théorèmes exposés au chapitre III et dans ce chapitre permettent, en se servant aussi du cas particulier d'un théorème dû à M. Deuring (6), d'écrire une inégalité concernant le rang de $V^{(Z^*)}$.

Soit $\mathfrak{F} = CG(p^\varphi)$ le champ de Galois (c'est-à-dire corps fini de caractéristique p) ayant p^φ éléments.

Soit $\lambda(\mathfrak{z}) = a_0 + a_1\mathfrak{z} + \ldots \ \ldots + a_j\mathfrak{z}^j$ un polynôme dans $CG(p)$ par rapport à une indéterminée $\mathfrak{z}$. Désignons par ce polynôme l'opérateur de $\mathfrak{F}$ qui transforme tout $\alpha \in \mathfrak{F}$ en $\alpha + a_1\alpha^p + \ldots + a_j\alpha^{p^j}$.

Le cas particulier du résultat de M. Deuring dont nous avons besoin est :

Il existe un $\beta \in \mathfrak{F}$ *tel que pour tout* $\alpha \in \mathfrak{F}$ *on peut trouver un polynôme* $\lambda_\alpha(\mathfrak{z})$ *de manière que* $\alpha = \lambda_\alpha(\mathfrak{z}) \cdot \beta$.

F étant un diviseur de φ, posons $\mathfrak{z}^F = \mathfrak{Z}$. Regardons les seuls opérateurs de $\mathfrak{F}$ qui sont représentés par les polynômes en $\mathfrak{Z}$ [dans $CG(p)$]. Si l'on pose

$$\beta_i = \mathfrak{z}^i \cdot \beta \qquad (i = 0, 1, \ldots, F-1), \tag{20}$$

tout $\alpha \in \mathfrak{F}$ se représente sous la forme

$$\alpha = \lambda_0^{(\alpha)}(\mathfrak{Z}) \cdot \beta_0 + \lambda_1^{(\alpha)}(\mathfrak{Z}) \cdot \beta_1 + \cdots + \lambda_{F-1}^{(\alpha)}(\mathfrak{Z}) \cdot \beta_{F-1}. \tag{21}$$

(6) *Mathematische Annalen*, 1932-1933, t. 107, pp. 140-144.

Soit M un sous-module de $\mathfrak{s}$ qui admet $\mathfrak{Z}$ comme opérateur. Soit q un des nombres 0, 1, ..., F — 1. Les éléments de M de la forme

$$\lambda_0(\mathfrak{Z})\,\beta_0 + \lambda_1(\mathfrak{Z})\,\beta_1 + \cdots + \lambda_q(\mathfrak{Z})\,\beta_q \tag{22}$$

forment encore un module admettant $\mathfrak{Z}$ comme opérateur. Il en résulte que les $\lambda_q^{(\alpha)}(\mathfrak{Z})$ de tels $\alpha \leqslant M$ forment un idéal, soit $(r_q(\mathfrak{Z}))$. Il existe donc un $\alpha \leqslant M$ tel que

$$\lambda_q^{(\alpha)}(\mathfrak{Z}) = r_q(\mathfrak{Z}) \qquad \text{et} \qquad \lambda_i^{(\alpha)}(\mathfrak{Z}) = 0 \quad \text{si} \quad i > q. \tag{23}$$

Désignons cet α par α_q. On vérifie aisément que tout $\alpha \leqslant M$ peut se mettre sous la forme

$$\lambda_0(\mathfrak{Z})\,\alpha_0 + \lambda_1(\mathfrak{Z})\,\alpha_1 + \cdots + \lambda_{F-1}(\mathfrak{Z})\,\alpha_{F-1}. \tag{24}$$

Désignons, comme précédemment, par F le degré absolu de $\mathfrak{P}$ dans K. On a

Lemme 7. On peut trouver un sous-hypergroupe $G^{(Z^*)}_{K/\overline{K}}$ de $V^{(Z^*)}_{K/k}(\mathfrak{P})$ du rang $\leqq F$ tel que $i_0 > 0$.

Démonstration. Soit δ_0 le dénominateur de v_0; soit π' un nombre tel que $\pi'^{\delta_0} = \pi$, où π est un nombre de K d'ordre 1 en $\mathfrak{P}$, et soit K^* un surcorps Galoisien de K par rapport à k contenant π'; alors $M_0(K/k;\ \pi',\ \mathfrak{P}^*)$ admet $\mathfrak{Z}$ comme opérateur (car $\gamma^* = 1$) et est un sous-module d'un corps fini de caractéristique p, par exemple, du corps de classes de restes (mod $\mathfrak{P}^*$) dans K^*. Donc il y a F éléments de $M_0(K/k;\ \pi',\ \mathfrak{P}^*)$, $\alpha_0, \alpha_1, \ldots$ ..., α_{F-1} tels que tout élément de cet ensemble se met sous la forme $\lambda_0(\mathfrak{Z})\,\alpha_0 + \lambda_1(\mathfrak{Z})\,\alpha_1 + \ldots + \lambda_{F-1}(\mathfrak{Z})\alpha_{F-1}$.

Choisissons dans $V_{K/k}(\mathfrak{P}^*)$ F éléments $\sigma_0, \sigma_1, \ldots$ ..., σ_{F-1} tels que $\beta_0(\sigma_i;\ \pi',\ \mathfrak{P}^*) = \alpha_i$. Soit $G^{(Z^*)}_{K/\overline{K}}$ le moindre sous-hypergroupe de $V^{(Z^*)}$ qui les contient tous. Donc $\mathfrak{R}(G^{(Z^*)}_{K/\overline{K}}) \leqq F$. $M_0(K/\overline{K};\ \pi',\ \mathfrak{P}^*)$ contient les α_i $(i = 0,\ 1, \ldots$ ..., F — 1) et admet $\mathfrak{Z}$ comme opérateur. Donc $M_0(K/\overline{K};\ \pi',\ \mathfrak{P}^*)$ contient tous les éléments de $M_0(K/k;\ \pi'\ \mathfrak{P}^*)$, donc lui est égal. Par conséquent, $\rho_0 = r_0$ et $i_0 > 0$. C. Q. F. D.

Théorème 13. $\mathfrak{R}[V_{K/k}\ (\mathfrak{P}^*)^{(Z^*)}] \leqq c_0 r_{-1}(K/k;\ \mathfrak{P})\ DF + 1$, où D est le plus petit commun dénominateur de tous les $v_q(K/k;\ \mathfrak{P})$ $(q = 0,\ 1, \ldots, m - 1)$.

Démonstration. Tous les nombres de cette formule étant les mêmes pour K/k et $K(\mathfrak{P})/k(\mathfrak{p})$, supposons K/k local. Nous allons déterminer une suite $U_1 = \{1_K\}$, $U_2 U_3, \ldots \ldots, U_{n+1} = V_{K/k}$ de sous-hypergroupes de $V_{K/k}$ tels que $U_1 < U_2 < U_3 < \ldots \ldots < U_{n+1}$, de la manière suivante : U_j étant déterminé, soit ω_j le plus petit indice tel que $U_j \overset{(\omega_j+1)}{V}_{K/k}$ ne contient pas $\overset{(\omega_j)}{V}_{K/k}$. Soit u_j le plus petit nombre tel qu'on puisse prendre dans $\overset{(\omega_j)}{V}_{K/k}$ u_j éléments $\sigma_{j,1}$, $\sigma_{j,2}$, ..., σ_{j,u_j} tels que l'hypergroupe U'_j engendré par U_j et ces éléments satisfasse à $U'_j \overset{(\omega_j+1)}{V}_{K/k} \geqq \overset{(\omega_j)}{V}_{K/k}$.

On pose $U_{j+1} = U'_j$.

Il est clair que $\mathfrak{R}(U_j) \leqq u_1 + u_2 + \ldots \ldots + u_{j-1}$. Soit $K^{(j)}$ le corps appartenant à U_j dans K et soit $v^{(j)} = v_0(K^{(j)}/k; \mathfrak{P}^*)$. Il est clair que $i_0(\mathfrak{P}; K, K^{(j)}, k) = \omega_j$ et que $\omega_{j+1} > \omega_j$. Il en résulte que $i^{(j)} = i_0(K^{(j)}, K^{(j+1)}, k) > 0$; d'où

$$v^{(j+1)} = v_0(K^{(j)}/k) + \sum_{q=1}^{i^{(j)}} \frac{v_q(K^{(j)}/k) - v_{q-1}(K^{(j)}/k)}{d_q(K^{(j)}/k)} > v_0(K^{(j)}/k) = v^{(j)}.$$

En vertu du théorème 2 de ce chapitre, tous les $v^{(j)}$ ont les dénominateurs égaux à ceux de v_{ω_j} correspondants, donc diviseurs de D. Comme, d'après le théorème 9, $v^{(j)} \leqq e_0 d_0 (K^{(j)}/k) \frac{p}{p-1} = e_0 r_{-1}(K/k) \frac{p}{p-1}$ et, sauf si $v^{(j)} = e_0 r_{-1} \frac{p}{p-1}$, on a $v^{(j)} \not\equiv 0 \pmod{p}$, $v^{(j)}$ ne peut prendre que

$$\left[e_0 d_0 D \frac{p}{p-1}\right] - \left[\frac{\left[e_0 d_0 D \frac{p}{p-1}\right]}{p}\right] = e_0 d_0 D_0,$$

valeurs $\not\equiv 0 \pmod{p}$, et encore, si le corps de Galois K^*/k de K/k contient toutes les racines p-ièmes de l'unité, la valeur $e_0 r_{-1} \frac{p}{p-1}$. Donc toujours $n \leqq e_0 d_0 D + 1$.

Déterminons u_j. Supposons d'abord que $j \neq e_0 d_0 D$. On peut choisir dans $V_{K^{(j)}/k}$ un ensemble $\{\bar{\sigma}_1, \bar{\sigma}_2, \ldots, \bar{\sigma}_s\}$ avec $s \leqq F$ tel que l'hypergroupe $\overline{U}$ qu'engendrent les éléments de cet ensemble ait $i_0 \neq 0$. $\mathrm{gen}._K \overline{U}$ est un sous-hypergroupe de $V_{K/k}$ et si $\sigma_i \leqslant \mathrm{gen}._K \bar{\sigma}_i$ $(i = 1, 2, \ldots, 0)$, $\mathrm{gen}._K \overline{U}$ est engendré par les σ_i $(1 = 1, 2, \ldots, 3)$ et l'hypergroupe $U_j = G_{K/K^{(j)}}$; puisque $\mathrm{gen}._K \overline{U}$. $\overset{(\omega_j+1)}{V}_{K/k} \geqq \overset{(\omega_j)}{V}_{K/k}$, on a $u_j \leqq s \leqq F$.

Supposons maintenant $j = e_0 d_0 D + 1$, c'est-à-dire $(v^{(j)} \equiv 0 \pmod p)$; théorème 10 de ce chapitre montre que $r_0(K^{(j)}/k) = p$, c'est-à-dire si $\bar\sigma$ est dans $V_{K^{(j)}/k}$ et non dans $\overset{(1)}{V}_{K^{(j)}/k}$, l'hypergroupe engendré par $\bar\sigma$ a $\rho_0 = p = r_0$ et $i_0 > 0$; donc $\sigma \leqslant \text{gen.}_K \bar\sigma$ et U_j engendrent U_{j+1} ; d'où $u_j = 1$.

Par conséquent, $\mathfrak{R}(V^{(Z^*)}_{K/k}) \leqq e_0 r_{-1} D.F + 1$. C. Q. F. D.

Complément. Si tous les v_q ont les numérateurs divisibles par un même entier θ (naturellement $(\theta, D) = 1$), θ divise aussi tous les $v^{(j)}$, et la démonstration précédente montre que

$$\mathfrak{R}(V^{(Z^*)}_{K/k}) \leqq e_0 r_{-1} F \frac{D}{\theta} + 1. \tag{25}$$

Conséquence. Si K/k est galoisien, on a $D = 1$; donc $\mathfrak{R}[V_{K/k}(\mathfrak{P})] \leq e_0 r_{-1}(K/k ; \mathfrak{P}) F + 1$; le signe d'égalité ne peut avoir lieu que si $K(\mathfrak{P})$ contient toutes les racines p- ièmes de l'unité.

Théorème 14. Si $v_0(K/k ; \mathfrak{P}) \equiv 0 \pmod p$, $\mathfrak{R}(V_{K/k}(\mathfrak{P}^*)^{(Z^*)}) = 1$.

Démonstration. Soit σ un élément de $V_{K/k}$ de niveau 0 et soit $G_{K/\overline{K}}$ l'hypergroupe engendré par σ. D'abord, $r_0 = p$ et $\rho_0 > 1$, on a $r_0 = \rho_0$. Soit que $G_{K/\overline{K}} \neq V_{K/k}$.

Alors $\overline{K}/k$ a un nombre de ramification propre $v_0(\overline{K}/k ; \overline{\mathfrak{P}})$, et, puisque $i_0 > 0$, on a

$$v_0(\overline{K}/k ; \overline{\mathfrak{P}}) > v_0(K/k ; \mathfrak{P}) = e_0 r_{-1} \frac{p}{p-1},$$

ce qui est impossible

Donc, $G_{K/\overline{K}} = V_{K/k}$ et $\mathfrak{R}(V^{(Z^*)}_{K/k}) = 1$.

Conséquence. Si K/k est galoisien et $v_0 \equiv 0 \pmod p$, $V_{K/k}$ est cyclique. En effet, les seuls groupes dont le rang est 1 sont les groupes cycliques. Ce théorème a été démontré pour la première fois par M. Öystein Ore (3).

CHAPITRE V

CORPS HASSIENS

1° Définitions.

Définition 1. Un corps K/k s'appelle *Hassien* ou *de type* H *(pour* $\mathfrak{P}$*)*, si pour tout $q = 0, 1, \ldots, m-1$ v_q est entier et

$$v_q \equiv v_{q-1} \pmod{d_q}. \tag{1}$$

La congruence précédente se décompose en deux congruences : une modulo $\frac{d_q}{d_0}$ (qui est une puissance de p) et l'autre modulo d_0 (qui est premier à p). Conformément à cela, j'introduis deux notions, dont celle des corps Hassiens est l'intersection.

Définition 2. Un corps K/k s'appelle *de type* H' *(pour* $\mathfrak{P}$*)*, si pour tout $q = 0, 1, \ldots \ldots, m-1$

$$v_q \equiv v_{q-1} \left(\mathrm{mod}\ \frac{d_q}{d_0}\right). \tag{2}$$

Définition 3. Un corps K/k s'appelle *de type* H'' *(pour* $\mathfrak{P}$*)*, si tous les v_q $(q \equiv 0, 1. \ldots, m-1)$ sont entiers et divisibles par d_0.

L'ordre et le degré absolus de l'idéal $\mathfrak{p}$ de k seront désignés par e_0, f_0, ceux de $\mathfrak{P}$ seront désignés par E, F; enfin, comme toujours, e, f désignent l'ordre et le degré de $\mathfrak{P}$ dans K/k. Si K/k est du type H, ou H', ou H'' et $e_0 = 1$, le corps K sera dit corps de type resp. H, ou H', ou H'' *absolu*.

2° Théorème 1. — Si K/k est du type H, ou H', ou H'' pour $\mathfrak{P}$ et si $\overline{\mathrm{K}}/k$ est un sous-corps de K/k, $\overline{\mathrm{K}}/k$ est resp. du type H, ou H', ou H'' pour $\overline{\mathfrak{P}}$.

Démonstration :

$$\overline{v}_q - \overline{v}_{q-1} = \sum_{j=i_{q-1}+1}^{i_q} \frac{v_j - v_{j-1}}{\Delta_j} = \sum_{j=i_{q-1}+1}^{i_q} \frac{d_j}{\Delta_j} \frac{v_j - v_{j-1}}{d_j} = \overline{d}_q \sum_{j=i_{q-1}+1}^{i_q} \frac{v_j - v_{j-1}}{d_j}$$

Si K/k est du type H', $\sum_{j=i_{q-1}+1}^{i_q} \frac{v_j - v_{j-1}}{d_j}$ a le dénominateur premier à p; donc $v_q \equiv v_{q-1} \left(\mathrm{mod}\ \frac{\bar{d}_q}{\bar{d}_0}\right)$, et $\overline{K}/k$ est du type H'; si K/k est du type H'', le dénominateur de $\sum_{j=i_{q-1}+1}^{i_q} \frac{v_j - v_{j-1}}{d_j}$ est une puissance de p; donc $\bar{v}_q - \bar{v}_{q-1}$ est, d'après le théorème de chapitre IV, entier et se divise par $\overline{d}_0$ et $\overline{K}/k$ est du type H''.

C. Q. F. D.

Théorème 2. Si le sous-corps K/k d'un corps K/k est du type H, ou H', ou H'' et si, pour tout $q = 0, 1, \ldots \ldots, m-1$, on a $\rho_q < r_q$; K/k est du type resp. H, ou H', ou H''.

Démonstration. On a, dans l'hypothèse de l'énoncé, pour tout q, $i_q = q$. Donc $\bar{v}_q - \bar{v}_{q-1} = \frac{v_q - v_{q-1}}{\Delta_q}$; si $v_q - v_{q-1} \equiv 0 \left(\mathrm{mod}\ \frac{\bar{d}_q}{\bar{d}_0}\right)$, on a

$$v_q - v_{q-1} \equiv 0 \left(\mathrm{mod}\ \frac{\overline{d}_q}{\overline{d}_0}\frac{\Delta_q}{\Delta_0} = \frac{d_q}{d_0}\right),$$

et si $\bar{v}_q - \bar{v}_{q-1}$ est entier et divisible par $\overline{d}_0$, $v_q - v_{q-1}$ est entier et divisible par $\overline{d}_0 \Delta_0 = d_0$. D'où le théorème.

3° M. Helmut Hasse (1) a démontré un théorème [dont une partie a été démontrée antérieurement par M. Masao Suguwara (2)], conséquence de son *Führer-Diskriminantensatz,* qui peut être formulé ainsi :

Théorème de Hasse. Si $T_{K/k}(\mathfrak{P}^*)$ est un groupe Abelien, K/k est de type H pour $\mathfrak{P}$.

Je suis dans l'impossibilité de reproduire ici la démonstration de ce théorème, basée sur la théorie locale des corps de classes. On pourra la trouver dans les mémoires cités de M. Hasse.

---

(1) La première démonstration de ce théorème a été donnée par M. Hasse dans un mémoire de *Journ. f. d. reine und ang. Math.*, 1930, t. 162, pp. 169-184, précédemment cité. M. Hasse l'a mise sous forme plus simple dans un mémoire de *Journ. of Fac of Sc.*, Tokyô, 1934, t. 2, pp. 477-498.

(2) Proc. Imp. Acad., Tokyô, t. 2, 1926, pp. 366-367.

G étant un groupe, désignons par G_c son groupe de commutateurs. Alors a lieu le

Théorème 3. Si K/k est un corps galoisien tel que $[T_{K/k}(\mathfrak{P})]_c$ (regardé comme $G_{K/\overline{K}}$) a tous ses $\rho_q < r_q$ $(q = 0, 1, \ldots \ldots, m-1)$, K/k est de type H pour $\mathfrak{P}$.

Démonstration. Comme $\overline{K}$ appartenant à T_c a $T_{\overline{K}/k} \simeq T_K/T_c$ groupe Abelien, $\overline{K}/k$ est du type H.

Le théorème s'obtient en appliquant aux K/k et $\overline{K}/k$ le théorème 2.

Conséquence 1. Tout sous-corps du corps K/k du théorème précédent est du type H : cela suit du théorème 1.

Il est évident, que si $K/\overline{K}$ est du type H′ pour $\mathfrak{P}$ et si l'ordre de $\mathfrak{P}$ dans $\overline{K}/k$ est premier à p, K/k est du type H′ pour $\mathfrak{P}$. Il en résulte la

Conséquence 2. Si K/k est galoisien et $[V_{K/k}(\mathfrak{P})]_c$ (regardé comme $G_{K/\overline{K}}$) a tous ses $\rho_q < r_q$, ou si K/k est un sous-corps d'un tel corps, K/k est du type H′ pour $\mathfrak{P}$.

3° Corps du type H″.

Théorème 4. Si K_1/k est tel que $\mathfrak{P}_1$ est d'ordre puissance de p dans K_1/k et n'a que des nombres de ramification entiers et si K_2/k est tel que $\mathfrak{P}_2$ est d'ordre premier à p dans K_2/k, $K = (K_1, K_2)$ désignant le corps composé de K_1, K_2 et $\mathfrak{P} \mid (\mathfrak{P}_1, \mathfrak{P}_2)$, K/k est de type H″ pour $\mathfrak{P}$.

Démonstration. K_1/k est de type H″ pour $\mathfrak{P}$, parce que $d_0(K_1/k; \mathfrak{P}_1) = 1$. D'autre part, l'ordre de $\mathfrak{P}$ dans K/K_1 est premier à p, parce que autrement $V_{K/K_1}(\mathfrak{P}^*)$ ne se réduirait à $\{1_K\}$ et $V_{K_2/k}(\mathfrak{P}^*) \geq \text{corr.}_{K_2} V_{K/K_1}(\mathfrak{P}^*)$ ne se réduirait pas à $\{1_{K_2}\}$. Donc pour tout q (si l'on pose $K_1 = \overline{K}$) on a $\rho_q = 1 < r_q$; d'où le théorème (3).

(3) Dans le cas de K/k galoisien, ce théorème a été démontré par Herbrand (*Journ. d. Math. p. et appl.*, 1931, t. 96, p. 481-498).

Dans le cas du K/k galoisien ce théorème admet le réciproque suivant :

Théorème 5. Si K/k galoisien est de type H'', il est composé des deux corps de la nature indiquée au théorème 4. Le groupe $T_{K/k}(\mathfrak{P})$ n'a qu'un seul sous-groupe d'ordre r_{-1} et ce sous-groupe appartient à son centre.

Démonstration. K_0 est r_{-1} — corps de ramification de K/k. Donc, il y un sous-groupe θ de $T_{K/k}$ d'ordre r_{-1}, engendré par un de ses éléments t, tel que $V_{K/k} = W(t)$. Les éléments de θ sont bien permutables avec tous les éléments de $T_{K/k} = \theta V_{K/k} = \theta . W(t)$. Comme tous les sous-groupes de $T_{K/k}$ d'ordre r_{-1} sont transformés de θ par des éléments de $V_{K/k}$, ils coïncident avec θ. K est le composé du corps qui appartient à θ et du corps K_0. Le théorème est démontré.

4° Rang des $\overset{(q)}{V}$ dans le corps de type H',

Théorème 6. Si K/k est de type H', on a, D étant le plus petit commun dénominateur et θ étant le p. g. c. d. premier à p des numérateurs de tous les $v_q(K/k; \mathfrak{P})$,

$$\Re\left(\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(Z^*)}\right) \leqq e_0 r_{-1}(K/k; \mathfrak{P})\, F\, \frac{D}{\theta}\frac{p}{p-1}. \tag{3}$$

Démonstration. Comme dans la démonstration du théorème 13 du chapitre IV, nous supposerons K/k local.

Considérons le corps K/K_q; dans ce corps l'hypergroupe de ramification est $\overset{(q)}{V}_{K/k}$. Procédons avec ce corps, comme nous l'avons fait avec K/k dans la démonstration du théorème 14. Les corps $K^{(s)}$ qu'on obtiendra seront, d'après le théorème 1 de ce chapitre, toujours de type H' par rapport à k; donc, toujours $v^{(s)} \equiv v_{q-1}\left(\mathrm{mod}\ \frac{d_q}{d_0}\right)$. Distinguons deux cas : 1) $v_{q-1} \not\equiv 0 \pmod p$; alors les $v^{(s)}$ doivent être parmi les fractions de dénominateur D et du numérateur divisible par θ et $\equiv D r_{q-1}\left(\mathrm{mod}\ \frac{d_q}{d_0} = \frac{d_q}{r_{-1}}\right)$ et $v^{(s)} \leqq e_0 d_q \frac{p}{p-1}$; donc, le nombre des $v^{(s)}$ ne dépasse pas

$$E\frac{e_0 d_q D\,\frac{p}{p-1}\cdot r_{-1}}{\theta d_q} + 1; \qquad \text{donc} \qquad \Re\left(\overset{(q)}{V}{}^{(Z^*)}_{K/k}\right) \leqq e_0 r_{-1}\, F\, \frac{D}{\theta}\frac{p}{p-1};$$

2) $v_{q-1} \equiv 0 \pmod p$; alors $v_q \equiv v_{q-1}\left(\mathrm{mod}\ \frac{n_0}{n_q}\right)$, donc aussi $(\mathrm{mod}\ p)$, donc $v_q \equiv 0 \pmod p$. D'après le théorème 14 du chapitre IV, $\Re\left(\overset{(q)}{V}{}^{(Z^*)}_{K/k}\right) = 1$. Théorème est démontré.

Lemme 1. Si $i_q^{(j)} = i_0(\mathfrak{P}; \mathrm{K}, \mathrm{K}^{(j)}, k)$, les $\mathrm{K}^{(j)}$ désignant les mêmes corps que dans la démonstration précédente (c'est-à-dire relatifs à K/K_q et non à K/k!), on a

$$i_q^{(n)} \leqq e_0 r_{-1}(\mathrm{K}/k; \mathfrak{P}) \frac{\mathrm{D}}{\theta} \frac{p}{p-1} + q - 1. \tag{4}$$

Démonstration. On a, quand on pose $\mathrm{K}^{(n)} = \overline{\mathrm{K}}$,

$$\bar{v}_q = v^{(n)} = \sum_{j=0}^{i_q^{(n)}} \frac{v_j - v_{j-1}}{\Delta_j} = v_{q-1} - v_{-1} + \sum_{j=q}^{i_q^{(n)}} \frac{v_j - v_{j-1}}{\Delta_j},$$

car $\Delta_0 = \Delta_1 = \ldots \quad \ldots = \Delta_{q-1} = 1$.

Or $\frac{d_j}{d_q} \equiv 0 \pmod{\Delta_j}$, $\frac{v_j - v_{j-1}}{\Delta_j} \equiv 0 \left(\mathrm{mod}\ \theta \frac{d_q}{d_0}\right)$; donc $\frac{v_j - v_{j-1}}{\Delta_j} \geqq \frac{\theta}{\mathrm{D}} \frac{d_q}{d_0}$ et

$$v^{(n)} \geqq v_{q-1} + (i_q^{(n)} + 1 - q) \frac{\theta}{\mathrm{D}} \frac{d_q}{d_0},$$

et, puisque $v^{(n)} \leqq e_0 d_q \frac{p}{p-1}$, on a

$$i_q^{(n)} + 1 \leqq q + \frac{\mathrm{D}}{\theta} e_0 d_0 \frac{p}{p-1}. \qquad \text{C. Q. F. D.}$$

Désignons par $G^{(a)}$ le groupe engendré par les puissances a-ièmes de tous les éléments d'un groupe G.

Théorème 7. K/k étant un corps galoisien de type H′ dont tous les nombres de ramification pour $\mathfrak{P}$ sont divisibles par θ, $(\theta, p) = 1$, on a

$$\left((\overset{(q)}{\mathrm{V}}_{\mathrm{K}/k}(\mathfrak{P}))_c, (\overset{(q)}{\mathrm{V}}_{\mathrm{K}/k}(\mathfrak{P})^{(p)})\right) \geqq \overset{\left(q + \left[\frac{e_0 r_{-1}}{\theta} \frac{p}{p-1}\right]\right)}{\mathrm{V}_{\mathrm{K}/k}}(\mathfrak{P}). \tag{5}$$

Démonstration. $\overset{(q)}{\mathrm{V}}_{\mathrm{K}/k}$ possède une base $\{\sigma_1, \sigma_2, \ldots \quad \ldots, \sigma_s\}$ dont tous les éléments ont les niveaux ne dépassant pas $i_q^{(n)}$ et telle que les éléments σ_i de cette base ayant le même niveau q ont les $\beta_q(\sigma_i)$ linéairement indépendants par rapport au corps fini de classes de restes rationnelles (mod $\mathfrak{P}$). Parmi toutes les bases de $\overset{(q)}{\mathrm{V}}$ ayant ces deux propriétés, extrayons celles qui contiennent le nombre minimum d'éléments de niveau q; soit x_0 ce nombre; parmi les bases de $\overset{(q)}{\mathrm{V}}$ ainsi obtenus extrayons celles dont le nombre d'éléments de niveau $q+1$ est minimum : soit x_1 ce nombre; parmi celles-ci extrayons les bases dont le

nombre d'éléments de niveau $q+2$ est minimum. Poursuivons ce procédé jusqu'à niveau $i_q^{(n)}$ (au delà, d'après la première condition à laquelle satisfont les bases regardées, il n'y a pas d'éléments de bases qu'on a extraites). Nous arrivons à un ensemble des bases de $\overset{(q)}{\mathrm{V}}$ dont nous prenons une

$$\left\{ \sigma_1, \sigma_2, \ldots, \sigma_{x_0+x_1+\cdots+x_{i_q^{(n)}-q}} \right\} \tag{6}$$

où

$$\lambda(\sigma_q) = j \quad \text{si} \quad \sum_{s=0}^{j-1} x_s < q \leqq \sum_{s=0}^{j} x_s.$$

Ceci posé, soit que

$$\prod_{q=1}^{\eta} \sigma_q^{\gamma_q} = \mathrm{C}\sigma, \quad \text{avec} \quad \lambda(\sigma) \geqq i_q^{(n)} + 1 \quad \text{et} \quad \mathrm{C} \leqslant \overset{(q)}{\mathrm{V}}_c. \tag{7}$$

(Le symbole $\overset{\curvearrowleft}{\prod}_{q=1} \alpha_q$, où les α_q ne sont pas supposés permutables entre eux dans la multiplication, signifie $\alpha_1 \alpha_2 \ldots \alpha_\kappa$. Voir : Van der Waerden : ***Moderne Algebra***, t. I, p.).

Montrons qu'alors $\gamma_1 \equiv \gamma_2 \equiv \ldots \ldots \equiv \gamma_\eta \equiv 0 \pmod{p}$. En effet, d'abord, on peut écrire, μ étant un quelconque des nombres 1, 2, ..., η.

$$\mathrm{C} = \mathrm{C}_1 \mathrm{C}_2, \tag{8}$$

où C_1 est un produit des commutateurs d'éléments de la base autres que σ_μ et C_2 est un produit des commutateurs de σ_μ par les autres éléments σ_q de la base, des commutateurs de ces commutateurs par les σ_q, des commutateurs d'éléments ainsi obtenus par les σ_q, etc., donc, d'après la conséquence du lemme 2 du chapitre IV, $\lambda(\mathrm{C}_2) \geqq \lambda(\sigma_\mu) + 1$.

Il en résulte que $\lambda(\mathrm{C}_2\sigma) \geqq \lambda(\sigma_\mu) + 1$; on peut écrire l'égalité (7) sous la forme suivante :

$$\sigma_\mu^{\gamma_\mu} = \left(\prod_{q=1}^{\mu-1} \sigma_q^{\gamma_q} \right)^{-1} \cdot \mathrm{C}_1 \cdot \mathrm{C}_2\sigma \cdot \left(\prod_{q=\mu+1}^{\eta} \sigma_q^{\gamma_q} \right)^{-1}. \tag{9}$$

Si $\gamma_\mu \not\equiv 0 \pmod{p}$, σ_μ, dont l'ordre est une puissance de p, est une puissance de $\sigma_\mu^{\gamma_\mu}$. Donc

$$\{ \sigma_1, \sigma_2, \ldots, \sigma_{\mu-1}, \sigma_{\mu+1}, \ldots, \sigma_\eta, \mathrm{C}_2\sigma \} \tag{10}$$

est encore une base de $\overset{(q)}{\mathrm{V}}$; d'ailleurs, si $\lambda(\mathrm{C}_2\sigma) > i_q^{(n)}$, d'après la démonstration du théorème 6 et du lemme 1, $\{\sigma_1, \sigma_2, \ldots, \sigma_{\mu-1}, \sigma_{\mu+1}, \ldots \ldots, \sigma_\eta\}$ est déjà une

base de $\overset{(q)}{V}$ (car, autrement, le corps appartenant au groupe engendré par ces éléments aurait v_0 ne satisfaisant pas au théorème 9 du chapitre IV). Par conséquent, $\overset{(q)}{V}$ possède une base satisfaisant aux conditions indiquées et qui a x_0 éléments de niveau q, x_1 éléments de niveau $q+1$, ..., ..., $x_{\lambda(\sigma_\mu)-1-q}$ éléments de niveau $\lambda(\sigma_\mu)-1$, et $x_{\lambda(\sigma_\mu)-q}-1$ éléments de niveau $\lambda(\sigma_\mu)$, contre l'hypothèse que $x_{\lambda(\sigma_\mu)-q}$ est le nombre minimum d'éléments de ce niveau que peut posséder une telle base. Donc $\gamma_\mu \not\equiv 0 \pmod p$ est impossible, et comme cela a lieu pour chaque $\mu = 1,2, \ldots \ldots, \eta$, on a bien $\gamma_1 \equiv \gamma_2 \equiv \ldots \ldots \equiv \gamma_\eta \equiv 0 \pmod p$.

Prenons maintenant un élément quelconque σ de $\overset{\left(q+\left[\frac{e_0 r_{-1}}{\theta}\frac{p}{p-1}\right]\right)}{V}$. Comme $q+\frac{e_0 r_{-1}}{\theta}\frac{p}{p-1} \geqq i_q^{(n)}+1$, on a $\lambda(\sigma) > i_q^{(n)}$. Puisque $\{\sigma_1, \sigma_2, \ldots \ldots, \sigma_\eta\}$ est une base de $\overset{(q)}{V}$, on peut toujours présenter σ sous la forme

$$\sigma = C^{-1}\prod_{q=1}^{\eta}\sigma_q^{\gamma_q} \qquad \text{où } C^{-1}, \text{ donc aussi } C \leqslant \overset{(q)}{V}_c; \tag{11}$$

il en résulte $\prod_{q=1}^{\eta}\sigma_q^{\gamma_q} = C\sigma$, et d'après ce qui précède, on a $\gamma_1 \equiv \gamma_2 \equiv \ldots \ldots \equiv \gamma_\eta \equiv 0 \pmod p$.

Donc

$$\prod_{q=1}^{\eta}\sigma_q^{\gamma_q} \leqslant \overset{(q)}{V}^{(p)} \qquad \text{et} \qquad \sigma \leqslant (\overset{(\sigma)}{V}_c, \overset{(q)}{V}^{(p)}). \qquad \text{C. Q. F. D.}$$

5° Corps hassiens absolus. — Nous allons maintenant démontrer un certain nombre de résultats sur les nombres de ramification et sur la structure des $\overset{(q)}{V}$ des corps de type H *absolus*.

Théorème 8. Si K est hassien absolu, *a*) sauf si à la fois $p=2$ et les v_q sont pairs

$$v_q = \sum_{j=0}^{q} d_j \; (q = -1, 0, \ldots, m-1) \quad b) \text{ si } p = 2 \text{ et les } v_q \text{ sont pairs, } v_q = d_{q+1} = 2^{q+1} r_{-1}.$$

Remarque. Puisque pour $q>0$, $d_q \equiv 0 \pmod p$, tous les v_q propres d'un corps hassien absolu sont congrus entre eux (mod p). En particulier, si $p=2$, les v_q sont ou bien tous pairs, ou bien tous impairs.

Démonstration du théorème 8. Puisque K est hassien absolu, $e_0 = 1$. Donc

$$v_q \leqq d_q \frac{p}{p-1} \leqq 2d_q \qquad (q = 0, 1, \ldots, m-1), \tag{12}$$

où le deuxième signe d'égalité n'a lieu que si $p = 2$. D'autre part, d'après la définition même des corps hassiens,

$$v_q \equiv v_{q-1} \pmod{d_q}. \tag{13}$$

Si $q > 0$, donc $v_{q-1} > 0$, on a ou bien $v_q - v_{q-1} = d_q$, ou bien $v_q \geqq 2d + v_{q-1} > 2d_q$, ce qui est impossible, parce que contredit l'égalité (12); donc $v_q - v_{q-1} = d_q$. Si $q = 0$, on a $v_0 \equiv 0 \pmod{d_0}$, donc ou bien $v_0 = d_0$, ou bien, puisque $v_0 \leqq 2d_0$, $v_0 = 2d_0$, ce qui ne peut avoir lieu, d'après une remarque précédente, que si $p = 2$. Si $v_0 = 2d_0$, les v_q sont pairs et l'on est bien dans le cas *b*). Si $p = 2$ et $v_0 = d_0$, v_0 est impair, et aussi tous les v_q le sont, et l'on est dans le cas *a*).

Supposons donc que nous sommes dans le cas *a*). Alors, pour tout $q = 0, 1, \ldots \ \ldots, m-1$, on a $v_q - v_{q-1} = d_q$; d'où

$$v_q = v_q - v_{-1} = \sum_{j=0}^{q} (v_j - v_{j-1}) = \sum_{j=0}^{q} d_j \tag{14}$$

Supposons que nous sommes dans le cas *b*). Les v_q étant tous pairs, on a, d'après le théorème 10 du chapitre IV, $r_q = p = 2$ pour tout $q \geqq 0$. Donc $d_q = 2^q d_0 = 2^q r_{-1}$. On a $v_0 = 2d_0$ et, pour $q = 1, 2, \ldots \ \ldots, m-1$, $v_q - v_{q-1} = d_q = 2^q r_{-1}$. D'où

$$\left\{ \begin{aligned} v_q &= v_0 + (v_q - v_0) = v_0 + \sum_{j=1}^{q} (v_j - v_{j-1}) = 2d_0 + \sum_{j=1}^{q} d_j \\ &= r_{-1}\left(2 + \sum_{j=1}^{q} 2^j\right) = 2^{q+1} r_{-1} = d_{q+1}. \end{aligned} \right. \tag{15}$$

C. Q. F. D.

Théorème 9. Si K est un corps hassien absolu et $\bar{K}$ est un sous-corps de K tel que $\rho_q = r_q$, *a*) sauf si $q = 0$, $p = 2$ et les v_q sont impairs, pour tout $j \leqq q$, on a $\rho_j = r_j$ 2) si $q = 0$, $p = 2$ et les v_q sont impairs, ou bien tous les $\rho_j = r_j$ $(j = 0, 1, \ldots, m-1)$, ou bien les $\bar{v}_q$ sont pairs.

Démonstration. Il suffit de démontrer le théorème en supposant que q est le plus petit nombre tel que $\rho_q = r_q$. Supposons qu'il y ait $j > q$ tel que $\rho_j \neq r_j$. Alors

$$q < i_q < m \quad \text{et} \quad \bar{v}_q - \bar{v}_{q-1} = \sum_{j=i_{q-1}+1}^{i_q} \frac{v_j - v_{j-1}}{\Delta_j} = \sum_{j=q}^{i_q} \frac{v_j - v_{j-1}}{\Delta_j} > \frac{v_{i_q} - v_{i_q-1}}{\Delta_{i_q}} = \frac{d_{i_q}}{\Delta_{i_q}} = \bar{d}_q.$$

Comme $\overline{\mathrm{K}}$ est hassien absolu, pour $q > 0$ et aussi pour $q = 0$, à l'exception du cas où $p = 2$ et les $\bar{v}_q$ sont pairs, $\bar{v}_q - \bar{v}_{q-1} = \bar{d}_q$, et l'on a une contradiction.

Supposons $q = 0$, $p = 2$; alors, si les v_q sont pairs, on a

$$\bar{v}_0 = \sum_{j=0}^{i_0} \frac{v_j - v_{j-1}}{\Delta_0} > \frac{v_0 - v_{-1}}{\Delta_0} = \frac{2d_0}{\Delta_0} = 2\bar{d}_0$$

contre le théorème que $\bar{v}_0 \leqq 2\bar{d}_0$; donc, dans le cas a) on a bien, pour $j \geqq q$, $\rho_j = r_j$; dans le cas b), si cela n'a pas lieu, les $\bar{v}_q$ sont pairs. C. Q. F. D.

Théorème 10. Si K est hassien absolu, sauf quand $q = 0$, $p = 2$ et les v_q sont impairs,

$$\mathfrak{R}\left(\overset{(q)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P}^*)^{(\mathrm{Z}^*)}\right) = \mathfrak{R}\left(\left(\overset{(q)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P}^*) \Big/ \overset{(q+1)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P})\right)^{(\mathrm{Z}^*)}\right) \leqq \mathrm{F}. \tag{16}$$

Dans le cas exceptionnel indiqué

$$\mathfrak{R}\left(\left(\overset{(q)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P}^*) \Big/ \overset{(q+1)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P}^*)\right)^{(\mathrm{Z}^*)}\right) \leqq \mathfrak{R}\left(\overset{(q)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P}^*)^{(\mathrm{Z}^*)}\right) \leqq \mathfrak{R}\left(\left(\overset{(q)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P}^*) \Big/ \overset{(q+1)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P}^*)^{(\mathrm{Z}^*)}\right) + 1 \leqq \mathrm{F} + 1. \tag{17}$$

Démonstration. Tout d'abord le rang de $\left(\overset{(q)}{\mathrm{V}} \Big/ \overset{(q+1)}{\mathrm{V}}\right)^{(\mathrm{Z}^*)}$ ne dépasse pas celui de $\overset{(q)}{\mathrm{V}}^{(\mathrm{Z}^*)}$. En effet, si $\{\sigma_1, \sigma_2, \ldots, \sigma_r\}$ est une base du rang minimum de $\overset{(q)}{\mathrm{V}}^{(\mathrm{Z}^*)}$ on a pour chaque $\sigma \leqslant \overset{(q)}{\mathrm{V}}$

$$\sigma \leqslant \sigma_{i_1}\sigma_{i_2} \ldots \sigma_{i_\mu}, \tag{18}$$

où $\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_\mu}$ sont certains (non obligatoirement inégaux deux à deux) des $\sigma_1, \sigma_2, \ldots, \sigma_r$. Soit $\bar{\sigma}$ un élément de $\left(\overset{(q)}{\mathrm{V}} \Big/ \overset{(q+1)}{\mathrm{V}}\right)^{(\mathrm{Z}^*)}$ et posons $\bar{\sigma}_i = \sigma_i \overset{(q+1)}{\mathrm{V}}$ (la loi de composition étant celle de $\overset{(q)}{\mathrm{V}}^{(\mathrm{Z}^*)}$). Si σ est un élément de $\overset{(q)}{\mathrm{V}}$ qui est dans $\bar{\sigma}$, on peut écrire

$$\sigma \overset{(q+1)}{\mathrm{V}} < \sigma_{i_1}\sigma_{i_2} \ldots \sigma_{i_\mu} \overset{(q+1)}{\mathrm{V}} < \sigma_{i_1} \overset{(q+1)}{\mathrm{V}} \cdot \sigma_{i_2} \overset{(q+1)}{\mathrm{V}} \ldots \sigma_{i_\mu} \overset{(q+1)}{\mathrm{V}},$$

c'est-à-dire

$$\bar{\sigma} \leqslant \bar{\sigma}_{i_1}\bar{\sigma}_{i_2} \ldots \bar{\sigma}_{i_\mu} \tag{19}$$

et $\{\bar{\sigma}_1, \bar{\sigma}_2, \ldots \ \ldots, \bar{\sigma}_r\}$ est une base de $(\overset{(q)}{\mathrm{V}} / \overset{(q+1)}{\mathrm{V}})^{(Z^*)}$, ce qui démontre l'affirmation.

Ceci posé, reprenons la démonstration du théorème 14 du chapitre IV. On voit que pour K/K_q, on a, d'après le théorème 9 de ce chapitre, $\mathrm{K}^{(2)} = \mathrm{K}_q$ dans le cas général, et que ou bien $\mathrm{K}^{(2)} = \mathrm{K}_q$, ou bien $\mathrm{K}^{(2)}/\mathrm{K}_q$ a les nombres de ramification pairs, c'est-à-dire, d'après le théorème 15 du chapitre IV, $u_1 = 1$, dans le cas exceptionnel. D'après la même démonstration, $u_1 \leqq \mathfrak{R}[(\overset{(q)}{\mathrm{V}} / \overset{(q+1)}{\mathrm{V}})^{(Z^*)}] \leqq \mathrm{F}$.

Donc dans le cas général, $\mathfrak{R}\,\overset{(q)}{\mathrm{V}}{}^{(Z^*)} = u_1 \leqq \mathfrak{R}\,[(\overset{(q)}{\mathrm{V}} / \overset{(q+1)}{\mathrm{V}})^{(Z^*)}]$; et comme il est aussi $\geqq \mathfrak{R}\,[(\overset{(q)}{\mathrm{V}} / \overset{(q+1)}{\mathrm{V}})^{(Z^*)}]$, on a bien $\mathfrak{R}\,\overset{(q)}{\mathrm{V}}{}^{(Z^*)} = \mathfrak{R}\,[(\overset{(q)}{\mathrm{V}} / \overset{(q+1)}{\mathrm{V}})^{(Z^*)}]$. Dans le cas exceptionnel on a, si $\mathrm{K}^{(2)} \neq \mathrm{K}_q$ (quand $\mathrm{K}^{(2)} = \mathrm{K}_q$, on a l'égalité précédente), $\mathfrak{R}\,[\mathrm{V}^{(Z^*)}] = u_1 + 1$, ce qui démontre le reste du théorème.

Conséquence. Si K/k est galoisien, $\mathfrak{R}\,(\overset{(q)}{\mathrm{V}} / \overset{(q+1)}{\mathrm{V}}) = l_q$; donc, si K est encore hassien absolu, $\mathfrak{R}\,(\overset{(q)}{\mathrm{V}}_{\mathrm{K}}) = l_q$ ou (dans le cas exceptionnel) $l_q + 1$.

Théorème 11. Si K/k est galoisien et hassien absolu, sauf si $q=0$, $p=2$, $v_q \equiv/\equiv 0 \pmod 2$,

$$(20) \qquad \big((\overset{(q)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P}))_c,\ (\overset{(q)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P}))^{(p)}\big) = \overset{(q+1)}{\mathrm{V}}_{\mathrm{K}}(\mathfrak{P})\ (4).$$

Démonstration. On a $\mathfrak{R}\,(\overset{(q)}{\mathrm{V}}) = l_q$. Donc, si $\{\sigma_1, \sigma_2, \ldots \ \ldots, \sigma_{l_q}\}$ est une base de $\overset{(q)}{\mathrm{V}}$, $\sigma_1, \sigma_2, \ldots \ \ldots, \sigma_{l_q}$ sont indépendants (mod $\overset{(q+1)}{\mathrm{V}}$), c'est-à-dire $\sigma_1^{\gamma_1}\sigma_2^{\gamma_2}\ldots \ \ldots \sigma_q^{\gamma}$ n'est dans $\overset{(q+1)}{\mathrm{V}}$ que si tous les $\sigma_i^{\gamma_i}$ $(i = 1, 2, \ldots, l_q)$ y sont. Soit $\sigma \leqslant \overset{(q+1)}{\mathrm{V}}$. Puisque $\sigma_1, \sigma_2, \ldots \ \ldots, \sigma_{l_q}$ est une base de $\overset{(q)}{\mathrm{V}}$, σ se représente $\sigma = \sigma_1^{\gamma_1}\sigma_2^{\gamma_2}\ldots\sigma_{l_q}^{\gamma_{l_q}}.\sigma_c$, où $\sigma_c \leqslant \overset{(q)}{\mathrm{V}}_c.\sigma_c$ est dans $\overset{(q+1)}{\mathrm{V}}$. Donc $\sigma_1^{\gamma_1}\sigma_2^{\gamma_2}\ldots \ \ldots \sigma_{l_q}^{\gamma_{l_q}} \equiv 1_{\mathrm{K}} \pmod{\overset{(q+1)}{\mathrm{V}}}$; donc $\gamma_1 \equiv \gamma_2 \equiv \ldots \ldots \equiv \gamma_{l_q} \equiv 0 \pmod p$ et $\sigma \leqslant (\overset{(q)}{\mathrm{V}}_c, \overset{(q)}{\mathrm{V}}{}^{(p)})$. Comme $\overset{(q)}{\mathrm{V}}_c$ et $\overset{(q)}{\mathrm{V}}{}^{(p)}$ sont dans $\overset{(q+1)}{\mathrm{V}}$, le théorème est démontré.

---

(4) Ce que $(\overset{(q)}{\mathrm{V}}_c, \overset{(q)}{\mathrm{V}}{}^{(p)}) \geqq \overset{(q+1)}{\mathrm{V}}$ est, pour $p > 2$, un cas particulier du théorème 7 de ce chapitre; en effet, si l'on y pose $e_0 = 1$ et $\theta = r_{-1}$, $q + \left[e_0 \frac{r_{-1}}{\theta} \frac{p}{p-1}\right]$ devient $q + \left[\frac{p}{p-1}\right]$, qui est égal, quand $p > 2$, à $q + 1$.

NOTES COMPLÉMENTAIRES

NOTE 1. (Au théorème 21 du chapitre II).

Théorème. Il existent des corps K/k tels que dans K il y ait un idéal premier $\mathfrak{P}$ de manière que le corps de décomposition de $\mathfrak{P}$ dans K/k n'existe pas.

Démonstration. Démontrons d'abord qu'il existe un groupe d'ordre fini G ayant un sous-groupe g tel que pour la période θ d'un certain élément de G on ait $\theta g \neq g\theta$. Supposons que ce n'est pas vrai. Alors, pour chaque groupe G, chaque sous-groupe g de G et chaque sous-groupe cyclique θ de G on doit avoir $\theta g = g\theta$. Soit g_1 n'importe quel autre (égal ou inégal à g) sous-groupe de G. Si γ est un élément quelconque de g_1 et si Γ est la période de cet élément, on a $\gamma g \leq \Gamma g = g\Gamma \leq g g_1$ et $g\gamma \leq g\Gamma = \Gamma g \leq g_1 g$; donc $g_1 g = g g_1$ et $g g_1$ est un groupe.

Il en résulte, par la méthode connue, que (parce que $(g_1 g_2 : g_2) = (g_1 : (g_1 \wedge g_2))$, si K_1/k, K_2/k sont deux corps quelconques, $K = (K_1, K_2)$, $k_0 = K_1 \wedge K_2$,

$$(K : K_2) = (K_1 : k_0). \tag{1}$$

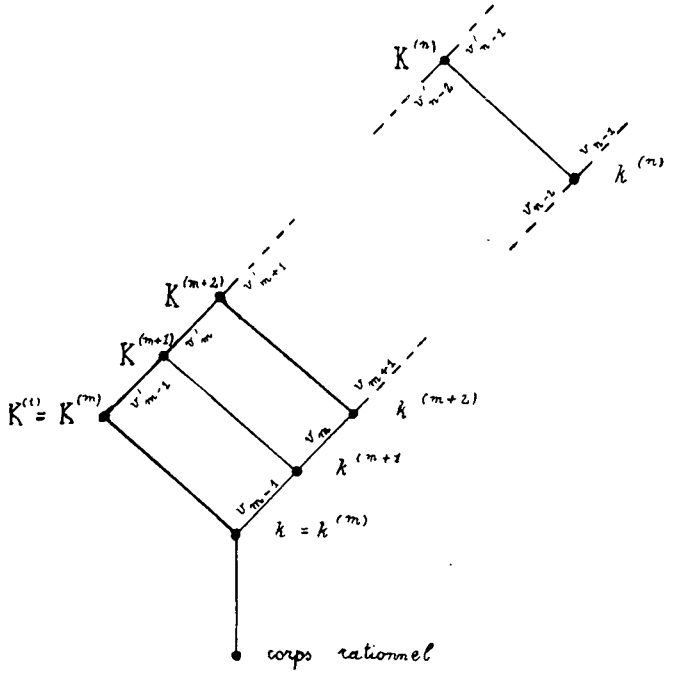
Or, prenons pour K_1, K_2 deux corps conjugués de degré n et sans affect (il en existe, d'après un théorème de M. Hilbert). $K_1 \wedge K_2 = k_0$ est le corps rationnel; le degré de $K = (K_1, K_2)$ est $n(n-1)$. Donc on doit avoir $n(n-1) : n = n : 1$, c'est-à-dire $n - 1 = n$, ce qui est impossible.

La démonstration précédente montre déjà qu'on peut choisir K^*/k Galoisien tel que $G_{K^*/k}$ possède un sous-groupe g et un sous-groupe cyclique θ tels que $\theta g \neq g\theta$, c'est-à-dire tels que θg ne soit pas un groupe. Posons $g = G_{K^*/K}$. D'après une loi des densités de Frobenius, il existe dans K^* des idéaux $\mathfrak{P}^*$ tels que $Z_{K^*/k}(\mathfrak{P}^*) = \theta$. Il en résulte que gen.$_{K^*} Z_{K/k}(\mathfrak{P}^*) = Z_{K^*/k}(\mathfrak{P}^*)$. $g = \theta g$ n'est pas groupe. C. Q. F. D.

NOTE 2. — (Au chapitre V).

Lemme. K étant un corps de nombres algébriques quelconque, $k^{(n)}$ étant le corps de racines p^n-ièmes de l'unité, $\mathrm{K}^{(n)}$ désignant $(\mathrm{K}, k^{(n)})$, $\mathfrak{p}^{(n)}$ désignant l'idéal premier de $k^{(n)}$ divisant p, $\mathfrak{P}$ désignant un idéal premier de K divisant p et $\mathfrak{P}^{(n)}$ désignant l'idéal premier de $\mathrm{K}^{(n)}$ divisant $\mathfrak{P}$, il existe un n tel que le plus grand nombre de ramification propre de $\mathfrak{P}^{(n)}$ dans $\mathrm{K}^{(n)}$ n'est pas parmi ceux de $\mathfrak{P}^{(n)}$ dans $\mathrm{K}^{(n)}/k^{(n)}$.

Démonstration. Soit $k = k^{(m)}$ le plus grand $k^{(n)}$ contenu dans $\mathrm{K}^{(1)}$.



Si $n \geq m$, $k^{(n+1)}/k^{(n)}$ et $\mathrm{K}^{(n+1)}/\mathrm{K}^{(n)}$ sont cycliques de degré p. $k^{(n+1)}/k^{(n)}$ est complètement ramifié par rapport à $\mathfrak{p}^{(n+1)}$, et le seul nombre de ramification propre de cet idéal dans $k^{(n+1)}/k^{(n)}$ est $v_{n-1} = p^n - 1$. $\mathrm{K}^{(n+1)}/\mathrm{K}^{(m)}$ est cyclique de degré p^{n+1-m}. Donc $\mathrm{T}_{\mathrm{K}^{(n+1)}/\mathrm{K}^{(m)}}(\mathfrak{P}^{(n+1)}) = \mathrm{V}_{\mathrm{K}^{(n+1)}/\mathrm{K}^{(m)}}(\mathfrak{P}^{(n+1)})$.

Il est impossible, si $p^{n+1-m} > (\mathrm{K}^{(1)} : k) = (\mathrm{K}^{(n+1)} : k^{(n+1)})$, que $\mathrm{K}^{(n+1)}/\mathrm{K}^{(m)}$ soit non ramifié pour $\mathfrak{P}^{(n+1)}$; car, alors, l'ordre de $\mathfrak{P}^{(n+1)}$ dans $\mathrm{K}^{(n+1)}/k$ ne dépasserait pas $(\mathrm{K}^{(1)} : k) < p^{n+1-m}$, ce qui est absurde. Donc, il existe j_0 tel que

si $n \geqq j_0$, $K^{(n+1)}/K^{(n)}$ est complètement ramifié pour $\mathfrak{P}^{(n+1)}$. Soit v'_{n-1} le seul nombre de ramification propre de $\mathfrak{P}^{(n+1)}$ dans $K^{(n+1)}/K^{(n)}$, si $K^{(n+1)}/K^{(n)}$ est ramifié pour $\mathfrak{P}^{(n+1)}$, et posons $v'_{n-1} = -1$ dans le cas contraire.

Soit s un entier tel que $p^s \geqq (K^{(1)} : k)$; alors $K^{(n)}/k^{(n)}$ a au plus s nombres de ramification différents. Posons $n = j_0 + s(q+1)$ $(q>0)$. $w_0, w_1, \ldots, w_r$ désignant tous les nombres de ramification propres de $\mathfrak{P}^{(n)}$ dans $K^{(n)}/k^{(n)}$ (donc $r \leqq s$), il y a i, $0 \leqq i \leqq r$ tel qu'il y ait q au moins de v'_c, $c \leqq n-1$ tels que $w_i < v'_c < w_{i+1}$. Les c satisfaisant à la condition écrite forment, évidemment, un ensemble d'entiers consécutifs. Soit σ un élément de $k^{(n)}/k^{(m)}$ tel que $v(\sigma ; \mathfrak{p}^{(n)}) = v_c$. Alors $\text{gen.}_{G_{K^{(n)}/K^{(m)}}} \sigma$ se réduit à l'ensemble contenant un seul élément σ' tel que $v(\sigma' ; \mathfrak{P}^{(n)}) = v'_c$. On a $\text{gen.}_{K^{(n)}} \sigma = \sigma'$. $G_{K^{(n)}/k^{(n)}}$. Il en résulte que le maximum de $v(\sigma'_1 ; \mathfrak{P}^{(n)})$ pour $\sigma'_1 \neq \text{gen.}_{K^{(n)}} \sigma$ est v'_c, car les éléments de $G_{K^{(n)}/k^{(n)}}$ ont les nombres caractéristiques qui sont soit $> v'_c$, soit $< v'_c$. Donc v'_c engendre v_c. Il en résulte, d'après les théorèmes de chapitre III, que pour au moins $q-1$ nombres consécutifs c on a

$$v_c - v_{c-1} = \frac{v'_c - v'_{c-1}}{d_i(K^{(n)}/k^{(n)} ; \mathfrak{P}_n)}, \text{ c'est-à-dire } v'_c - v'_{c-1} \geqq v_c - v_{c-1} = (p-1)p^c.$$

Or, soit que $w_r \geqq v'_{n-2}$. w_r engendre sûrement un nombre de ramification $\bar{w}$ de $\mathfrak{P}^{(1)}$ dans $K^{(1)}/k$. Ce nombre est

$$(1) \qquad \bar{w} = \frac{w_r - v'_{n-2}}{p^{n-j_0}} + \sum_{c=j_0-1}^{n-2} \frac{v'_c - v'_{c-1}}{p^{c-j_0+1}} \geqq p^{j_0-1} \sum_{c=j_0-1}^{n-2} \frac{v'_c - v'_{c-1}}{p^c} \geqq q(p-1)p^{j_0-1} \geqq q.$$

Si ε désigne le degré de $K^{(1)}$, on doit avoir $\bar{w} \leqq \frac{\varepsilon}{p-1}$. Donc, si l'on prend $n > j_0 + s\left(\frac{\varepsilon}{p-1} + 1\right)$, on a une contradiction qui démontre le théorème.

Généralisation. — Si $w_r < v'_{n-2}$, on en déduit que le plus grand nombre de ramification de $\mathfrak{P}^{(n-1)}$ dans $K^{(n-1)}/k^{(n-1)}$ est encore w_r. (Il suffit d'appliquer c, de 4° de la partie A du chapitre III). Il en résulte que si pour n_0 le lemme précédent a lieu, il en est de même pour tout $n > n_0$, et que w_r ne dépend pas de n quand $n > n_0$.

Donc, si $c \geqq n_0 - 2$, on a $v'_c > w_r$ et, ainsi, $v'_{c+1} - v'_c \geqq (p-1)p^{c+1}$. Il en résulte qu'à partir de n_0 les $K^{(n)}$ peuvent jouer le rôle des $k^{(n)}$ dans une démonstration analogue à celle du lemme précédent. Donc, en changeant un peu les notations on a le

Lemme. Il existe pour tout corps K/k un nombre n tel que le plus grand nombre de ramification de $\mathfrak{P}^{(n)}$ dans $K^{(n)}/k$ ne se trouve pas parmi ceux de $\mathfrak{P}^{(n)}$ dans $K^n/(k, k^{(n)})$.

Théorème. Il existe des corps K/k de type H pour un idéal $\mathfrak{P}$ tels que $T_{K/k}(\mathfrak{P})$ ne soit pas un groupe abelien.

Démonstration. Les corps galoisiens K/k n'ont pas tous les groupes $V_{K/k}(\mathfrak{P})$, pour tout $\mathfrak{P} \mid p$, abeliens.

En effet, autrement tous les corps seraient de type H′ pour tous les idéaux premiers de ces corps divisant p. Or, ε_2 désignant une racine p^2-ième primitive de l'unité, il est facile de vérifier que le corps de $\sqrt[p]{1-\varepsilon_2}$ a les nombres de ramification 0, $p-1$, p^2, $+\infty$, donc n'est pas de type H′ pour $(\sqrt[p]{1-\varepsilon_2}) \mid p$.

Ceci posé, on peut choisir un K/k tel que : 1) K/k soit galoisien, 2) $K^{(\mathfrak{P})}_0 = k$, 3) $V = V_{K/k}(\mathfrak{P})$ ne soit pas abelien ; 4) V_c soit d'ordre p et, si $\sigma \leqslant V_c$, $\lambda(\sigma) \geqq m-1$ (c'est-à-dire σ est du plus grand niveau possible ; $\lambda(\sigma) = m$ n'a lieu que si $\sigma = 1_K$) ; 1), 2), 3) sont évidentes. Supposons que 4) n'a pas lieu. Soit que $V^{(q-1)}_{K/k} > V_c \geqq V^{(q)}_{K/k}$.

Alors, si au lieu de K/k on prend K_q/k, il est évident (car $m = q$ dans K_q/k) que si $\sigma \leqslant V_c$, $\lambda(\sigma) \geqq m-1$.

En vertu de la conséquence du lemme 2 du chapitre IV, V_c est contenu dans le centre de V et, d'après le chapitre II, V_c est abelien de type $(p, p, \ldots, p)$. Donc, si au lieu de K on prend maintenant son sous-corps qui appartient à un sous-groupe Γ d'indice p de V_c, toutes les conditions exigées seront vérifiées.

Le corps K/k satisfaisant pour un $\mathfrak{P} \mid p$ aux conditions 1), 2), 3), 4) étant choisi, s'il est de type H′, tout est démontré. Sinon, composons K avec un $k^{(n)}$, où n est suffisamment grand pour que le plus grand nombre de ramification de $(K, k^{(n)})/k$ ne se trouve pas parmi ceux de $(K, k^{(n)})/(k, k^{(n)})$, ce qui est possible d'après le lemme précédent.

Soit K'/k le corps ainsi obtenu. Il est galoisien. Son groupe n'est pas abelien, car, autrement, son sous-corps K/k serait de type H′. Enfin, il a un sous-corps $\overline{K}' = (\overline{K}, k^{(n)})$, où $\overline{K}$ est le sous-corps de K appartenant à V_c, qui est abelien et tel que $(K' : \overline{K}') \mid (K : \overline{K}) = p$, d'où $(K' : \overline{K}') = p$. Le groupe $(T_{K'/k})_c$ est donc cyclique d'ordre p et, de plus, puisque $(T_{K'/k})_c \leq G_{K'/k^{(n)}}$, on a, quand $\sigma \neq 1_K$ est dans $(T_{K'/k})_c$, $-1 < \lambda(\sigma) < m'-1$. Donc, si σ' est un élément

de $T_{K'/k}$ tel que $\lambda(\sigma') = m' - 1$, donc appartenant au centre de $V_{K'/k}$, la période θ de $\sigma\sigma'$ n'est pas un surgroupe de $(T_{K'/k})_c = (V_{K'/k})_c$, est un sous-groupe invariant de $T_{K'/k}$, et le corps appartenant à θ a les mêmes ρ_q que celui qui appartient à $(T_{K'/k})_c$, c'est-à-dire le corps abelien K'/k.

Donc ce corps n'a ni le groupe T, ni même le groupe V abeliens, est galoisien, et a les mêmes v_q et d_q que $\overline{K}'/k$, c'est-à-dire est de type H. Le théorème est démontré.

Remarque. Si $p \neq 2$, il est certain que le groupe d'un corps galoisien hassien non abelien K/k n'est pas un groupe de Hamilton (1). Donc il possède des sous-groupes non-invariants et il y a des corps de type H dont $T^{(T^*)}_{K/k}$ (et même $V^{(V^*)}_{K/k}$) n'est pas groupe.

La même chose peut être démontrée d'une manière un peu plus compliquée pour $p = 2$.

Théorème. Il y a des corps K/k de type H' pour $\mathfrak{P}$ qui ne sont pas de type H'' pour le même idéal.

Démonstration. Soit k'/k un corps local tel que $n_{-1}(k'/k) = d_0(k'/k) > 1$. Prenons le plus grand corps abelien K/k' tel que son groupe ait le type $(p, p, \ldots, p)$. n' désignant la norme absolue de $\mathfrak{p}'$ dans k', d'après le *Führer-Discriminantensatz* de Hasse $v_0(K/k') = 1$, $v_1(K/k') - v_0(K/k') = n' \not\equiv 0 \pmod{d_0(k'/k) = d_0(K/k)}$; donc, quoique K/k soit de type H', il n'est pas de type H''.

Théorème. Il y a des corps K/k de type H'' qui ne sont pas de type H' pour le même idéal.

Démonstration. Le corps de $\sqrt[p]{1 - \varepsilon_2}$ de l'avant-dernier théorème est bien de type H'' pour $(\sqrt[p]{1 - \varepsilon_2})$ par rapport au corps de $\varepsilon_1 = \varepsilon_2^p$, car $d_0 = 1$ et $p - 1$, p^2 sont entiers, mais n'est pas de type H', car $p^2 \not\equiv p - 1 \pmod{\frac{d_1}{d_0} = p}$.

M. KRASNER.

---

(1) DEDEKIND, *Math. Ann.*, 1896, t. 48.

TABLE DES MATIERES

NOTES COMPLÉMENTAIRES

ERRATA

Page.	Ligne à partir du haut.	AU LIEU DE	LIRE
4	2	de corps	des corps
4	20	de corps	des corps
4	21	de corps	des corps
5	20	de cas galoisiens	du cas galoisien
5	21	d'idéaux	des idéaux
6	1	il existe	il existent
6	18	hypergroupes$_D$	des hypergroupes$_D$
6	23	Soit	Soient
6	25	),	).
6	26	soit	Soit
7	7	galoisiens	galoisien
10	16 à droite.	on a	on ait
11	2 à droite.	$\mathfrak{P}^* / \mathfrak{P}$	$\mathfrak{P}^* \mid \mathfrak{P}$
13	27	hypergroupe$_D$ K	hypergroupe$_D$ H
14	9 à gauche.	$\beta\ (\sigma_1\sigma_2 : \pi, \mathfrak{P})$	$\beta_q(\sigma_1\sigma_2 ; \pi, \mathfrak{P})$
14	28 à droite.	$\overset{(q+1)}{V}_{K/k}(\mathfrak{P}^*)^{(T*)}$	$\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(T*)}$
16	8 à droite.	$B_q(A ; \pi', \mathfrak{P}^*)$	$\beta\ (A ; \pi', \mathfrak{P}^*)$
16	15 à gauche.	Il existe	Il existent
16	16 à droite.	appelée	appelé
16	23 à droite.	resp.	resp. par
17	9	de corps	des corps
20	10	Théorème du chapitre III :	Le théorème du chapitre III,
20	12	d'existence	de l'existence
21	9	$\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(Z*}$	$\overset{(q)}{V}_{K/k}(\mathfrak{P}^*)^{(Z*)}$
21	10	du corps	d'un corps
21	12	et	et si
23	21	$c_1 c_2$	c_1, c_2
25	1	$\sum_{a_1 \leqslant A_1,\, a_1 \leqslant A_2} a_1 a_2$	$\sum_{a_1 \leqslant A_1,\, a_2 \leqslant A_2} a_1 a_2$
25	7	dans le sens	au sens
25	28	existe	existent
26	17-18	un hypergroupe	un sous-hypergroupe
26	28	et	et si
27	20	celui	celle

Page.	Ligne à partir du haut.	AU LIEU DE	LIRE
27	29	et	et si
28	9	et	et si
28	11	$= (\mathfrak{K}/h')_{\mathrm{D}}$	$= (\mathfrak{K}/h')_{\mathrm{D}}$
28	18	$= (\mathfrak{K}/h')_{\mathrm{D}}$	$= (\mathfrak{K}/h')_{\mathrm{D}}$
28	23	$h_2 (g_2/g)_{\mathrm{D}}$	$h_2 = (g_2/g)_{\mathrm{D}}$
34	2	et	et si
37	1	ensemble d'inertie	*ensemble d'inertie*
38	6	$n - 1$	$n = 1$
40	23	$u_0, u_1, \ldots, u_s$	$n_0, n_1, \ldots, n_s$
40	24	$0 \leqq u_0 < u_1 < \ldots < u_s < u$	$0 \leqq n_0 < n_1 < \ldots < n_s < u$
42	15	$\prod_{\sigma \ll g_{\mathrm{K}/k}} \sigma\mathfrak{P}$	$\prod_{\sigma \ll G_{\mathrm{K}/k}} \sigma\mathfrak{P}$
43	15	gen. σ	$\mathrm{gen.}_{\mathrm{Z}^*} \sigma$
43	25	nombres d'éléments $(\mathrm{Z}/\mathrm{T})^{(\mathrm{Z}^*)}$	nombres d'éléments de $(\mathrm{Z}/\mathrm{T})^{(\mathrm{Z}^*)}$
44	15	$\bar{\rho}^{p^{f_1 v_0}}$	$\bar{\rho}^{p^{2f_0}}$
44	21	appartient i;	appartient i [8];
45	1	auquelle	à laquelle
45	7	[1].	[9].
45	10	*et*	*et si*
47	13	(mod $\sigma\mathfrak{P}^2$)	(mod $\mathfrak{P}^{*2a}$)
47	24	théorème 10	le théorème 10
48	9	où $\sigma_1^* \leqslant \mathrm{gen.}_{\mathrm{T}^*} \sigma$,	où $\sigma_1^* \leqslant \mathrm{gen.}_{\mathrm{T}^*} \sigma_1$,
49	5	*Conséquence.*	*Conséquence* 2.
49	12	$(\mathrm{V}\sigma)^{(\cdot^*)}$	$(\mathrm{V}\sigma)^{(\mathrm{Z}^*)}$
50	17	$\sigma \geqslant \overset{(q)}{\mathrm{V}}$	$\sigma \leqslant \overset{(q)}{\mathrm{V}}$
51	1	il existe	il existent
51	12	*et*	*et si*
51	22	$\beta_q(\mathrm{V}; \pi', \mathfrak{P}^*)$	$\beta_q(\overset{(q)}{\mathrm{V}}; \pi', \mathfrak{P}^*)$
52	10	$\pi \equiv \alpha\pi^{*a}$	$\pi = \alpha\pi^{*a}$
53	3	$[\overline{\alpha^*}]_{\delta_q} = \overline{\alpha^*} \,.\, \mathfrak{E}_{\delta_q}$	$[\overline{\alpha^*}]_{\overline{\delta}_q} = \overline{\alpha^*} \,.\, \mathfrak{E}_{\overline{\delta}_q}$
53	8	$= 1$	$\equiv 1$
54	4	$+ [< \overline{\alpha}^{*-av_q} \beta_q(\sigma_2) >_{\mathrm{F}}]_{\delta_q}$	$+ [< \overline{\alpha}^{*-av_q} \beta_q(\sigma_2) >_{\mathrm{F}}]_{\overline{\delta}_q}$
54	9	$a + [< b >_{\mathrm{F}}]_{\delta_q}$	$a + [< b >_{\mathrm{F}}]_{\overline{\delta}_q}$
55	3	sous-hypergroupe $\mathrm{Z}^{(\mathrm{Z}^*)}$	sous-hypergroupe de $\mathrm{Z}^{(\mathrm{Z}^*)}$
56	5	$\mathrm{Z}_{\mathrm{K}/\mathrm{K}_\mathrm{Z}}(\mathfrak{P}^*) = \mathrm{T}_{\mathrm{K}/\mathrm{K}_\mathrm{Z}}(\mathfrak{P}^*) =$	$\mathrm{Z}_{\mathrm{K}/\mathrm{K}_q}(\mathfrak{P}^*) = \mathrm{T}_{\mathrm{K}/\mathrm{K}_q}(\mathfrak{P}^*) =$
57	3	galoisienne	une extension galoisienne
57	9	K/k	K^*/k
58	28	de K/k	de k
62	11	$r_q(\mathfrak{P}; \mathrm{K}/\mathrm{K})$	$r_q(\mathfrak{P}; \mathrm{K}/\overline{\mathrm{K}})$
62	15	de $\overset{(l)}{\nu}$,	de $\overset{(q)}{\nu}$
64	22	$\mathfrak{P}^{a\nu-1}$	$\mathfrak{P}^{*a\nu-1}$

Page.	Ligne à partir du haut.	AU LIEU DE	LIRE
64	28	$\sigma \leqslant G_{K/\overline{K}}$	$\sigma \leqslant G_{K/k}$
66	12	Galoisiens	galoisiens
66	22	non-Galoisiens	non-galoisiens
66	26	non-Galoisien	non-galoisien
67	1	Galoisien	galoisien
69	3	$q \geqq i$	$q \leqq i$
69	15	à automorphisme	à automorphisme de $G_{K/k}$
71	10	$\leqq t_{e_{s+1}} + s = 1$	$\leqq t_{e_{s+1}} + s + 1$
72	1	les nombres	les nombres non nuls
72	6	Kummeriens	kummeriens
72	15	Herband	Herbrand
74	2	K/k	$\overline{K}\ k$
75	3	$\sqrt[\overline{\delta}]{\overline{\pi}}$	$\sqrt[\overline{\delta}]{\overline{\pi}}$
76	1	$(\mathrm{mod}\ \overline{\mathfrak{p}}\mathfrak{P}^{a\overline{v}})$	$(\mathrm{mod}\ \overline{\mathfrak{p}}\mathfrak{P}^{a\overline{v}+1})$
77	5	M	M_q
77	6	M	M_q
77	13 (2 fois)	$\sum_{s=1}^{t_q}$	$\sum_{s=0}^{t_q}$
77	15	$\frac{\Delta'_{s+1}}{\Delta'_s}$	$\frac{\Delta'_{s+1}}{\Delta'_0}$
77	18	$\frac{v_{i_q}}{\Delta'_{s+1}} = \frac{v_{i_q}}{\rho_{-1}} \frac{\Delta'_0}{\Delta'_{s+1}}$	$\frac{v_{i_q}}{\Delta_{i_q}} = \frac{v_{i_q}}{\rho_{-1}} \frac{\Delta_0}{\Delta_{i_q}}$
77	18	$\frac{\rho_{-1}}{(v_{i_q}, \rho_{-1})} \cdot \frac{\Delta'_{s+1}}{\Delta_0}$	$\frac{\rho_{-1}}{(v_{i_q}, \rho_{-1})} \cdot \frac{\Delta_{i_q}}{\Delta_0}$
77	21	$\Delta_{i_q} \sum_{s=1}^{t_q} w_s \left(\frac{1}{\Delta'_s} - \frac{1}{\Delta_{s+1}}\right)$	$\Delta_{i_q} \sum_{s=0}^{t_q} w_s \left(\frac{1}{\Delta'_s} - \frac{1}{\Delta'_{s+1}}\right)$
78	26	Galoisien	galoisien
79	4	Galoisien	galoisien
80	24	Abelien	abelien
80	25	$\Psi_{j+1}/\Psi_j \sim$	$\Psi_{j-1}/\Psi_j \sim$
82	5	$\sigma_l = \tau_l^{h(l)} \sigma_l$	$\sigma_l \equiv \tau_l^{h(l)} \sigma_l$
82	19	$\sigma_{l+1} = \sigma_l \tau'$	$\sigma_{l+1} = \sigma_l \tau'_l$
82	23	$(\mathrm{mod}\ \overset{(l+1)}{V})$	$(\mathrm{mod}\ \overset{(q+1)}{V})$
82	28	, $\overline{m} - 1$	. $\overline{m} - 1$)
83	6	il y	il y a
85	25	$\sigma_{q+1} t \sigma_{q+1}^{-1} t^{-1}$	$\sigma_{q+1} t \sigma_{q+1}^{-1} t'^{-1}$
85	28	Théorème	Le théorème
86	17	;	,

Page.	Ligne à partir du haut.	AU LIEU DE	LIRE
88	19	$v_q \equiv \overline{v}_{q-1}$	$\overline{v}_q \equiv \overline{v}_{q-1}$
89	17	On a vu que	K/k étant galoisien, on a vu que
91	2	$\varphi_{i_q} + \sum_{j=i_{q-1}+1}^{i_q-1} \frac{p_j - 1}{r_j} \prod \frac{\rho_s}{r_s}$	$\varphi_{i_q} + \sum_{j=i_{q-1}+1}^{i_q-1} \frac{\rho_j - 1}{r_j} \prod_{s=j+1}^{i_q-1} \frac{\rho_s}{r_s}$
91	11	Abeliens	abeliens
94	1	c'est-à-dire ($v_j \equiv 0$	c'est-à-dire $v_j \equiv 0$
94	15	D'abord,	D'abord, puisque
95	4	*Hassien*	*hassien*
95	9	Hassiens	hassiens
96	4	théorème de chapitre IV	théorème 1 du chapitre IV
96	6	Si le sous-corps K/k	Si le sous-corps $\overline{\mathrm{K}}$/k
96	7	;	,
96	16	Abelien	abelien
97	6	Abelien	abelien
97	14	et	et si
98	28-29	Théorème	Le théorème
100	10	$\alpha_1 \alpha_2 \ldots \alpha_{\mathrm{K}}$	$\alpha_1 \alpha_2 \ldots \alpha_{,}$
100	12	p.)	p. 21)
102	23	et	et si
103	2	qu'il y ait $j > q$	qu'il y ait un $j > q$
104	5	$u_1 = 1$	$u_2 = 1$
105	22	Galoisien	galoisien
105	25	il existe	il existent
107	7	il y a i, $0 \leqq i \leqq r$ tel	il y a un i, $0 \leqq i \leqq r$, tel
108	4	Il existe	Il existent
108	6	les groupes	leur groupe
108	7	abeliens	abelien
108	15	Soit que $\overset{(q-1)}{\mathrm{V}}_{\mathrm{K}/k} > \mathrm{V}_c \geqq \overset{(q)}{\mathrm{V}}_{\mathrm{K}/k}$.	Soit que $\overset{(q-1)}{\mathrm{V}}_{\mathrm{K}/k}$, mais non $\overset{(q)}{\mathrm{V}}_{\mathrm{K}/k}$ contient (au sens large) V_c.