NOMBRE DES EXTENSIONS D'UN DEGRÉ DONNÉ D'UN CORPS $\mathfrak{P}$-ADIQUE

par Marc KRASNER
(Clermont-Ferrand)

INTRODUCTION

On sait que le corps réel **R** (et, également, tous les corps réels abstraits réellement clos) possède une propriété rare pour les corps non algébriquement clos : il possède une et une seule extension algébrique non triviale (le corps complexe $\mathbf{C} = \mathbf{R}(i)$, où $i^2 + 1 = 0$). Tant que je sache, on ne connaît pas d'autres corps [1] non algébriquement clos, qui n'ont qu'un nombre fini d'extensions algébriques. La plupart des corps usuels comme le corps des rationnels, les corps de nombres algébriques, les corps de fonctions algébriques d'une ou plusieurs variables etc, ont non seulement une infinité d'extensions algébriques, mais le nombre de leurs extensions reste infini si l'on en fixe le degré. Il se trouve que les corps $\mathfrak{p}$-adiques, c'est-à-dire les corps valués complets localement compacts de caractéristique 0, occupent, de ce point de vue, une position intermédiaire : bien que le nombre total des extensions algébriques d'un tel corps k soit infini, celui $\mathfrak{N}_{k,n}$ des extensions de k de degré n est fini pour tout n. Les corps des séries de puissances d'une variable sur un corps fini, qui sont les seuls corps valués complets localement compacts, mais de caractéristique $p \neq 0$, occupent encore une sorte de position intermédiaire entre les corps $\mathfrak{p}$-adiques et les corps quelconques, mais d'une manière où intervient l'Arithmétique. En effet, si le nombre $\mathfrak{N}_{k,n}$ des extensions de degré donné n de k est infini, par contre celui des extensions de degré et de différente donnés est fini.

[1] Le mot « corps » va signifier durant tout l'exposé « corps commutatif ».

Or il se trouve que non seulement on peut prouver que pour un corps valué localement compact k le nombre des extensions de degré et de différente donnés est fini et qu'il en est de même, dans le cas $\mathfrak{p}$-adique, pour celui $\mathfrak{N}_{k,n}$ des extensions de degré n de k, *mais il est possible de calculer explicitement ces nombres*, ainsi que les nombres des extensions d'un degré donné de k, qui possèdent, en plus, certaines propriétés algébrico-arithmétiques imposées, qui proviennent de la théorie de la ramification.

Le calcul des nombres des extensions mentionnées est basé sur une généralisation non abélienne de la théorie locale des corps de classes, s'appliquant, d'ailleurs, en partie aux extensions séparables de degré fini d'un corps valué complet quelconque. La première version de cette théorie, concernant uniquement le cas, où le corps de base est $\mathfrak{p}$-adique (et employant une technique beaucoup trop compliquée), a été donnée par l'auteur dans son travail [*1*] en 1937. Une version plus générale (s'appliquant, en principe, au corps de base valué complet quelconque) et mettant en évidence l'origine véritable de ses résultats, a été esquissée par l'auteur dans ses notes [*5*] des Comptes Rendus (1946-47) et dans ses conférences [*6*] (1949) et [7] (1950), mais n'a jamais été publiée sous une forme complète. L'idée fondamentale de cette théorie consiste à organiser l'ensemble S_k des polynomes unitaires irréductibles $\in k[x]$ en un espace ultramétrique à l'aide d'une distance convenable [on notera $S_{k,n}$ l'ensemble des $f \in S_k$ de degré n organisé par la même distance] et de faire correspondre à une extension séparable de degré fini K/k l'ensemble $\Sigma_{K/k}$ des $f(x) \in S_k$ définissant quelque surextension de K/k, considéré comme un sous-espace de l'espace ultramétrique S_k. Soit $\mathfrak{i}$ l'anneau de valuation de k. Il se trouve que la structure de $\Sigma_{K/k}$ ou de certaines de ses parties caractéristiques [telles l'ensemble $S_{K/k}$ des $f(x) \in S_k$ définissant K/k (qu'on peut caractériser comme l'ensemble des $f \in \Sigma_{K/k}$ dont le degré est le plus bas) et, dans le cas de valuation discrète, celui des $f \in S_{K/k} \cap \mathfrak{i}[x]$ et dont le discriminant est égal à celui de K/k (polynomes *discriminantiels*): on peut en citer d'autres encore] en tant que sous-espace de S_k, reflète de nombreux aspects de la structure algébrico-arithmétique de K/k, et tout particulièrement ses propriétés fournies par la théorie de la ramification. Grâce au principe suivant, dû à l'auteur (et qui est la véritable clé de cette théorie) :

Soient $\mathfrak{K}$ la clôture algébrique valuée de k, et $\alpha \in \mathfrak{K}$ un élément séparable sur k. Alors, si $\beta \in \mathfrak{K}$ est plus proche de α que de ses autres conjugués $\alpha' \neq \alpha$ par rapport à k, on a $k(\beta) \supseteq k(\alpha)$, on peut montrer que non seulement $\Sigma_{K/k}$ est ouvert, mais [en le combinant avec l'évaluation de $|f_{\alpha/k}(\beta)|$ [où $f_{\alpha/k}(x)$ est le polynome minimal de α sur k], qui n'est autre chose, au fond, que l'analogue dans l'Analyse valuée de la formule de croissance des fonctions entières dûe à Hadamard, qui équivaut, dans cette théorie, aux inégalités de Cauchy] on peut déterminer, pour une large classe de corps de base k (comprenant, en particulier, les corps valués localement compacts), en fonction des distances de α à ses autres conjugués ([2]) (c'est-à-dire à partir des propriétés ramificatives de K/k en α), le rayon ρ_f [où $f(x) = f_{\alpha/k}(x)$] du plus grand cercle C_f de centre f contenu dans $\Sigma_{K/k}$. On peut, plus généralement, décrire en termes des mêmes propriétés de K/k en α, certains invariants métriques et algébriques ([3]) du sous-espace $\Sigma_{K/k}$ de S_k autour de $f = f_{\alpha/k}$. Réciproquement, ces invariants donnent des informations assez riches sur la structure ramificative de K/k en α. Si l'on considère le suprémum $\rho_{K/k}$ de ρ_f quand f parcourt tous les polynomes $\in S_{K/k} \cap \mathfrak{i}[x]$, la généralisation adéquate (aux extensions séparables de degré fini quelconque d'un corps valué k quelconque [*3*]) du conducteur $\mathfrak{f}_{A/k}$ d'une extension abélienne séparable A d'un corps localement compact k est l'idéal $\mathfrak{f}_{K/k}$ de $\mathfrak{R}$ tel que $|\mathfrak{f}_{K/k}| = \rho_{K/k}$ [d'ailleurs, si k est discrètement valué, les polynômes discriminantiels de $S_{K/k}$ peuvent se caractériser comme les polynômes $f \in S_{K/k}$ à coefficients entiers dont ρ_f est maximal]. Et certains invariants limites de la structure de $\Sigma_{K/k}$ autour des $f \in S_{K/k} \cap \mathfrak{i}[x]$ quand $\rho_f \to \rho_{K/k}$ donnent des informations sur la structure ramificative intrinsèque de K/k. Ainsi, la partie de $S_{K/k}$, formée par les polynômes f dont le discriminant D_f a une valuation $|D_f|$ assez proche de celle $|D_{K/k}|$ du discriminant $D_{K/k}$ de K/k peut se partager en cercles $\subset S_{k,n}$ [où $n = (K:k)$ est le degré de K/k] dont le rayon est proche de $\rho_{K/k}$. En particulier, dans le cas de valuation discrète, où l'existence des éléments discriminantiels est certaine, l'ensemble $S^{(d)}_{K/k}$ de ces éléments se partage en cercles de $S_{k,n}$ de rayon $\rho_{K/k}$. Si k est localement compact, le nombre de ces cercles (ou des cercles de tout rayon $\rho \leqslant \rho_{K/k}$) est fini. Il est facile de montrer que

$$\rho_{K/k} \geqslant |\mathfrak{d}_{K/k}|^2 = |D_{K/k}|^{n/2},$$

où $\mathfrak{d}_{K/k}$ est la différente de K/k, autrement dit l'idéal de $\mathfrak{R}$ engendré par $D^{1/n}_{K/k}$ (cette définition ne s'applique qu'au cas où k est complet; une définition plus orthodoxe sera donnée plus loin). Ainsi, pour toute extension K/k de degré n et de différente $\mathfrak{d}$ et pour tout $\rho \leqslant |\mathfrak{d}|^2$, $S^{(d)}_{K/k}$ est une réunion de cercles de rayon ρ. En plus, si l'on fixe le degré résiduel f de K/k $\left(\text{ou son ordre de ramification } e = \dfrac{n}{f}\right)$, et, en particulier, pour les extensions K/k complètement ramifiées ($f = 1$), on constate que le nombre de ces cercles contenus dans $S^{(d)}_{\alpha/k}$ est proportionnel au nombre $l_{K/k}$ des corps conjugués de K dans $\mathfrak{K}/k$. On montre que ce nombre est

$$A(k, n, f, \mathfrak{d}, \rho)\, l_{K/k},$$

([2]) Ces distances étant comptées avec leurs ordres de multiplicité respectifs.

([3]) Car on peut définir une addition dans certaines partitions des circonférences de S_k.

où $\Lambda(k, n, f, \mathfrak{d}, \rho)$ est une constante facilement calculable en fonction des paramètres écrits. Ainsi, les $l_{K/k}$ corps qui ont la même image $S^{(d)}_{K/k}$ par l'application $K/k \to S^{(d)}_{K/k}$, ont, dans cette image, $\Lambda(k, n, f, \mathfrak{d}, \rho)\ l_{K/k}$ cercles de rayon ρ. Donc, le quotient du nombre $N(S^{(d)}_{K/k}, \rho)$ des cercles $C \subseteq S^{(d)}_{K/k}$ de rayon ρ par le nombre $l_{K/k}$ des extensions $\subset \mathfrak{K}/k$, dont il est l'image, est la constante $\Lambda(k, n, f, \mathfrak{d}, \rho)$, et tout se passe comme s'il y avait ce nombre de cercles par extension. Il en résulte deux conséquences. D'une part, si $S^{(d)}_{K/k}$ est donné, il suffit de compter les cercles $C \subseteq S^{(d)}_{K/k}$ de rayon ρ pour déterminer si K/k est galoisienne (et, même, combien elle a d'extensions conjuguées), car $N(S^{(d)}_{K/k}, \rho) : \Lambda(k, n, f, \mathfrak{d}, \rho)$ est $l_{K/k}$, et K/k est galoisienne si, et seulement si $N(S^{(d)}_{K/k}, \rho) = \Lambda(k, n, f, \mathfrak{d}, \rho)$. Ceci constitue la loi de limitation pour les extensions galoisiennes, et cette loi, sous une forme modifiée, s'applique au cas de k valué complet quelconque, car le phénomène de proportionnalité de $N(S^{(d)}_{K/k}, \rho)$ à $l_{K/k}$ subsiste d'une certaine manière dans le cas général, mais comme ce $N(S^{(d)}_{K/k}, \rho)$ est infini, il n'est pas possible de le mettre en évidence en comptant les cercles $C \subset S^{(d)}_{K/k}$, et c'est à partir de certains invariants de $S^{(d)}_{K/k}$ (en tant que sous-espace de $S_{n,k}$) ou de certains ensembles plus compliqués, qu'on peut définir un indice analogue à

$$N(S^{(d)}_{K/k}, \rho) : \Lambda(k, n, f, \mathfrak{d}, \rho)$$

du cas localement compact. D'un autre côté, si l'on arrive à calculer (et je l'ai réussi) le nombre $M(k, n, f, \mathfrak{d}, \rho)$ de cercles de rayon ρ en lesquels se décompose l'ensemble de tous les polynômes $f(x)$ définissant les éléments discriminantiels de quelque extension K/k de degré n, de degré résiduel f et différente $\mathfrak{d}$, il suffit de diviser ce nombre par $\Lambda(k, n, f, \mathfrak{d}, \rho)$ pour avoir le nombre de ces extensions. Dans le présent exposé, ce calcul sera fait dans le cas complètement ramifié ($f = 1$) et les nombres $\mathfrak{K}^{(r)}_{k,n}$, $\mathfrak{K}_{k,n}$ des extensions complètement ramifiées, respectivement quelconques, de k de degré n, se calculent par les sommations convenables à partir du nombre précédent.

Depuis 1947, grâce aux travaux de Šafarevič [*10*], Kawada, Demuškin, Koch, on a pu déterminer la structure du groupe de Galois $\mathfrak{G}_{\mathfrak{K}/k}$ (organisée par sa topologie de Krull) de la clôture algébrique $\mathfrak{K}$ d'un corps valué localement compact k par rapport à ce corps k. Or, $\mathfrak{K}_{k,n}$ n'est autre chose que le nombre des sous-groupes fermés de $\mathfrak{G}_{\mathfrak{K}/k}$ d'indice n. Il semblerait qu'on pourrait, en principe, calculer $\mathfrak{K}_{k,n}$ à partir de $\mathfrak{G}_{\mathfrak{K}/k}$. Mais la structure de $\mathfrak{G}_{\mathfrak{K}/k}$ est, en général, assez compliquée, et, à l'heure actuelle, un tel calcul paraît inabordable. Il s'y ajoute un fait un peu mystérieux qu'a mis en évidence le calcul explicite de $\mathfrak{K}_{k,n}$ (où k est $\mathfrak{p}$-adique) par d'autres méthodes : *$\mathfrak{K}_{k,n}$ dépend de moins de paramètres que $\mathfrak{G}_{\mathfrak{K}/k}$*. En effet, il se trouve que $\mathfrak{K}_{k,n}$ dépend uniquement de n, de la caractéristique p du corps résiduel $\bar{k}$ de k et du degré $n_0 = (k : \mathbf{Q}_p)$ de k par rapport au corps $\mathfrak{p}$-adique rationnel (c'est-à-dire le complété du corps rationnel $\mathbf{Q}$ par rapport à sa $\mathfrak{p}$-valuation) $\mathbf{Q}_p$, tandis que $\mathfrak{G}_{\mathfrak{K}/k}$ dépend de bien d'autres paramètres que p, n et n_0 [il dépend, en particulier, du degré résiduel $f_0 = (\bar{k} : \bar{\mathbf{Q}}_p)$ de $k/\mathbf{Q}_p$ et du plus grand entier l tel que k contient les racines p^l-ièmes primitives de l'unité]. Ainsi, des groupes $\mathfrak{G}_{\mathfrak{K}/k}$ de formes très différentes peuvent avoir, pour tout n, le même nombre $\mathfrak{N}_{k,n}$ de sous-groupes fermés d'indice n, et le calcul de $\mathfrak{N}_{k,n}$ à partir de $\mathfrak{G}_{\mathfrak{K}/k}$ se fait donc à partir de structures comportant de nombreux invariants, qui doivent s'éliminer au cours de calcul, ce qui est une indication de plus de ses probables complications et difficultés (supposant qu'on arrive un jour à le faire). Par contre, la théorie de Šafarevič permet de calculer le nombre des extensions d'un certain type, ce que ma théorie ne permet pas, du moins dans son état actuel. Il s'agit du nombre $\mathfrak{N}_k\,(g)$ des extensions galoisiennes $\mathrm{K}/k \subseteq \mathfrak{K}/k$ ayant, à isomorphisme près, le p-groupe donné g comme groupe de Galois $\mathfrak{G}_{\mathrm{K}/k}$ (voir [*10*]).

J'ai démontré les formules pour les nombres des extensions de k de degré et de différentes données et ceux pour $\mathfrak{N}_{k,n}^{(r)}$ et $\mathfrak{N}_{k,n}$ dans mes Notes [*9*] des Comptes Rendus (1962) (bien que la première de ces formules ait été déjà signalée dans [*5*, *6* et *7*]. La partie de l'exposé qui suit est, d'ailleurs, très proche du texte de ces Notes, à peu d'exceptions près. Mais déjà en 1937 (note [*2*]) j'ai énoncé les formules pour le nombre des extensions ayant certaines propriétés arithmétiques, par exemple le degré résiduel, les nombres de ramification et les ordres des hypergroupes de ramification donnés. Certaines propriétés algébriques de l'extension K/k [primitivité, caractère métagaloisien] peuvent se caractériser arithmétiquement comme je l'ai montré, pour le cas $\mathfrak{p}$-adique, dans mon travail [*4*] [et la théorie correspondante pour le cas général est esquissée dans ma note des Comptes Rendus, t. 220 (1945), p. 28-30], et les nombres $\mathfrak{N}_{k,n}^{(pr)}$ et $\mathfrak{N}_{k,n}^{(mg)}$ des extensions primitives et des extensions métagaloisiennes de degré donné d'un corps localement compact k peuvent, également, se calculer à l'aide de la même théorie. Ces nombres ont été indiqués dans ma note [*3*] de 1938, (mais d'une manière pas tout à fait exacte pour $\mathfrak{N}_{k,n}^{(mg)}$).

L'exposé de ces résultats exigeant trop de développements, j'y reviendrai dans une autre publication.

Notation. — Etant donné un espace ultramétrique E, le cercle circonférencié de E de centre $a \in \mathrm{E}$ et de rayon r sera noté $\mathrm{C}(a, r; \mathrm{E})$.

A et B étant deux ensembles, la différence ensembliste de A et de B (c'est-à-dire l'ensemble des x tels que $x \in \mathrm{A}$ et $x \notin \mathrm{B}$) sera notée $\mathrm{A} \dashv\!\vdash \mathrm{B}$ (voir page 98 du présent ouvrage, les motifs que j'ai de préférer cette notation à celles qui sont habituellement employées).

1° Soient k un corps valué localement compact, $\mathfrak{p}$ son idéal premier, $\bar{k}$ son corps résiduel, p' et p les caractéristiques de k et de $\bar{k}$, $q = p^{f_0}$ le nombre d'éléments du corps (qui est fini) $\bar{k}$, $\mathfrak{K}$ la clôture algébrique valuée de k, $\mathbf{Q}_p$ le corps p-adique rationnel et, dans le cas $\mathfrak{p}$-adique ($p' = 0$), $n_0 = (k : \mathbf{Q}_p)$. Si $\mathrm{K} \subset \mathfrak{K}$ est une extension séparable de k de degré donné n et si $\mathfrak{P}$ est son idéal premier, posons $(p) = \mathfrak{P}^{\mathrm{E}}$ (donc $\mathrm{E} = +\infty$ si $p' = p$ et est l'ordre de ramification de $\mathrm{K}/\mathbf{Q}_p$ si $p' = 0$) et $n = hp^m$, où h est premier à p. Si $\mathfrak{d}_{\mathrm{K}/k}$ est la différente de K/k, écrivons-la sous la forme $\mathfrak{p}\,\mathfrak{P}^{j-1}$, et appelons ρ la partie entière $[j : \mathrm{E}]$ de $j : \mathrm{E}$. M. Ö. Ore a montré [10] que si K/k est complètement ramifiée et si s est le plus grand entier $\leqslant m$ tel que $p^s \mid j$, on a $s\mathrm{E} \leqslant j \leqslant m\mathrm{E}$, et que si j satisfait à cette condition, il existe des extensions complètement ramifiées K/k de degré n, telles que $\mathfrak{d}_{\mathrm{K}/k} = \mathfrak{p}\,\mathfrak{P}^{j-1}$. Soient $\mathfrak{N}^{(r)}_{k,n,j}$ (où j satisfait à la condition d'Ore) le nombre des $\mathrm{K} \subset \mathfrak{K}$ de cette forme et, dans le cas $\mathfrak{p}$-adique, $\mathfrak{N}^{(r)}_{k,n}$ et $\mathfrak{N}_{k,n}$ les nombres des extensions complètement ramifiées respectivement quelconques $\mathrm{K} \subset \mathfrak{K}$ de k telles que $(\mathrm{K} : k) = n$. Posons $l_j = q - 1$ ou 1 selon que $j < m\mathrm{E}$ ou $j = m\mathrm{E}$, $\varepsilon(s) = p^{-1} + p^{-2} + \ldots + p^{-s}$, si s est un entier > 0, $\varepsilon(0) = 0$ et $\varepsilon(-1) = -\infty$.

Si k est $\mathfrak{p}$-adique, posons

$$\mathrm{N} = (\mathrm{K} : \mathbf{Q}_p) = nn_0.$$

On a alors les

Théorème 1 :

$$\mathfrak{N}^{(r)}_{k,n,j} = nl_j\, q^{\frac{\mathrm{E}}{p} + \frac{\mathrm{E}}{p^2} + \ldots + \frac{\mathrm{E}}{p^\rho} + \left[\frac{j - \rho\mathrm{E}}{p^{\rho+1}}\right]},$$

Théorème 2 : Si k est $\mathfrak{p}$-adique, $\mathfrak{N}^{(r)}_{k,n}$ et $\mathfrak{N}_{k,n}$ sont finis et l'on a

$$\mathfrak{N}^{(r)}_{k,n} = n \sum_{s=0}^{m} p^s \{ p^{\varepsilon(s)\mathrm{N}} - p^{\varepsilon(s-1)\mathrm{N}} \},$$

$$\mathfrak{N}_{k,n} = \Big(\sum_{d \mid h} d \Big) \Big(\sum_{s=0}^{m} \frac{p^{m+s+1} - p^{2s}}{p-1} \{ p^{\varepsilon(s)\mathrm{N}} - p^{\varepsilon(s-1)\mathrm{N}} \} \Big).$$

2° Soit k un corps valué complet, $| \ldots |$ sa valuation,

$$\omega(\ldots) = -\operatorname{Log} | \ldots |$$

son ordre valuatif, $\mathfrak{K}$ une clôture algébrique valuée de k, $G = \mathfrak{G}_{\mathfrak{K}/k}$ le groupe de Galois de $\mathfrak{K}/k$, S_k l'ensemble des polynomes unitaires irréductibles d'une variable x à coefficients dans k. Si $f(x)$, $g(x)$ sont $\in S_k$, notons $R(f, g)$ leur résultant. Au signe près, $R(f, g)$ coïncide avec le produit des $f(\beta)$, où β parcourt l'ensemble $Z(g)$ des zéros (répétés selon l'ordre de leur multiplicité) de $g(x)$ dans $\mathfrak{K}$, et aussi avec celui des $g(\alpha)$, où α parcourt l'ensemble (avec répétitions) $Z(f)$ analogue. Tous les $f(\beta)$, $\beta \in Z(g)$, sont conjugués par rapport à k et, puisque k est complet, ont une même valuation. D'où, n et n' désignant les degrés respectifs des $f(x)$, $g(x)$, on a

$$| R(f, g) | = | f(\beta) |^{n'} = | g(\alpha) |^{n}$$

pour tout $\beta \in Z(g)$ et tout $\alpha \in Z(f)$.

Soit
$$Z(f) = \{ \alpha = \alpha_1, \alpha_2, \ \ldots, \ \alpha_n \},$$

où α a été choisi d'avance et les autres zéros de $f(x)$ ont été rangés d'une manière telle que les distances $r_i = | \alpha_i - \alpha |$ croissent (au sens large) avec i. La suite $r_1 = 0, r_2, \ldots, r_n$ (4) ne dépend pas du choix de α, car, si $\alpha' \in Z(f)$, il existe un $\sigma \in G$ tel que $\alpha' = \sigma.\alpha$. Mais, k étant complet, tous les $\sigma \in G$ sont des isométries, et la distance $d(\sigma.\alpha_i, \alpha')$ est $= d(\alpha_i, \alpha) = r_i$. Ainsi, la distance minimale d'un $\alpha \in Z(f)$ aux zéros $\alpha' \neq \alpha$ de $f(x)$ ne dépend pas du choix de α et est, par suite, égale à la distance minimale $\Delta(f)$ des zéros distincts de $f(x)$ dans $\mathfrak{K}$.

Soit $\beta \in Z(g)$, et soit $\alpha = \alpha(\beta)$ un des zéros de $f(x)$ le plus proche de β. La distance $d(\beta, \alpha(\beta))$ ne dépend pas du choix de β. En effet, si $\beta' \in Z(g)$, il existe un $\sigma \in G$ tel que $\beta' = \sigma.\beta$ et $d(\beta', \sigma.\alpha) = d(\beta, \alpha)$ est la plus courte des distances $d(\beta', \sigma.\alpha') = d(\beta, \alpha')$, où α' parcourt $Z(f)$. Mais $\alpha' \to \sigma.\alpha'$ est une permutation des zéros de $f(x)$. Ainsi, $d(\beta, \alpha(\beta))$ est égale, pour tout $\beta \in Z(g)$, à la plus courte distance $\Delta(f, g)$ entre les zéros de $f(x)$ et ceux de $g(x)$. Si f, g, h sont $\in S_k$, et si $\beta(\alpha)$ et $\gamma(\alpha)$ sont

(4) Soit $K = k(\alpha)$. Les valeurs distinctes, écrites dans l'ordre croissant, que prend

$$\omega(\alpha - \alpha_i) = - \operatorname{Log} r_i$$

s'appellent *nombres caractéristiques* de K/k en α et sont notés

$$\nu^{(\alpha)}_{0, K/k}, \ \nu^{(\alpha)}_{1, K/k}, \ \ldots, \qquad \nu^{(\alpha)}_{m(\alpha), K/k} = +\infty.$$

On constate que les ensembles $V^{(\alpha)}_{q, K/k}$ des isomorphismes α de K/k dans $\mathfrak{K}$ tels que

$$\nu^{(\alpha)}(\sigma) = \omega(\sigma.\alpha - \alpha)$$

soit $\geqslant \nu^{(\alpha)}_{q, K/k}$ sont des sous-hypergroupes de l'hypergroupe de Galois $\mathfrak{G}_{K/k}$ de K/k (voir pour les définitions les travaux cités [1] et [6]). On notera $n^{(\alpha)}_{q, K/k}$ l'ordre de $V^{(\alpha)}_{q, K/k}$.

les zéros de $g(x)$ et de $h(x)$, qui sont parmi les plus proches d'un $\alpha \in Z(f)$,

$$\Delta(g, h) \leqslant d\left(\beta(\alpha), \gamma(\alpha)\right)$$

ne dépasse pas

$$\operatorname{Max}\left[d\left(\alpha, \beta(\alpha)\right),\ d\left(\alpha, \gamma(\alpha)\right)\right], \qquad \text{qui est} \quad = \operatorname{Max}\left[\Delta(f, g),\ \Delta(f, h)\right].$$

Si l'on pose

$$\alpha(\beta) = \alpha = \alpha_1,$$

$|f(\beta)|$ est le produit des $|\beta - \alpha_i|$. Par définition,

$$|\beta - \alpha_i| \quad \text{est} \quad \geqslant |\beta - \alpha(\beta)| = \Delta(f, g).$$

Or, si

$$r_i = |\alpha - \alpha_i| \quad \text{est} \quad < \Delta(f, g),$$

$|\beta - \alpha_i|$ ne dépasse pas Max $[|\beta - \alpha|, r_i]$, lequel est $\Delta(f, g)$,

d'où
$$|\beta - \alpha_i| = \Delta(f, g).$$

Et si $r_i > \Delta(f, g)$, on a

$$|\beta - \alpha_i| = |\alpha - \alpha_i| = r_j.$$

Ainsi, l'on a

$$|\beta - \alpha_i| = \operatorname{Max}[\Delta(f, g), r_i],$$

et $|f(\beta)|$ est le produit des Max $[\Delta(f, g), r_i]$ (5). Pour un $f \in S_k$ fixé,

(5) Appelons *polygone de ramification* de K/k en α le polygone de Newton $\Pi^{(\alpha)}_{k/K}$ de

$$f_{\alpha/k}(\alpha + x) = f(\alpha + x).$$

Si $\nu = \omega(\beta - \alpha)$, où $\alpha = \alpha(\beta)$, et si L_ν est la tangente à $\Pi^{(\alpha)}_{K/k}$ de pente $-\nu$, soit $\varphi^{(\alpha)}_{K/k}(\nu)$ l'ordonnée de l'intersection de L_ν avec l'axe des ordonnées. Alors, on constate facilement que l'expression précédente de $|f(\beta)|$ est $\operatorname{Exp}\left(-\varphi^{(\alpha)}_{K/k}(\nu)\right)$. Ceci n'est que l'expression des inégalités de Cauchy de l'Analyse valuée pour le polynôme $u(x) = f(\alpha + x)$, qui est, en général, $\omega\left(u(x)\right) \geqslant \varphi^{(\alpha)}_{K/k}\left(\omega(x)\right)$, mais devient l'égalité $\omega\left(u(x)\right) = \varphi^{(\alpha)}_{K/k}\left(\omega(x)\right)$ s'il n'existe aucun zéro z de u, qui soit « proche » de x, autrement dit tel que $|x - z| < |x|$. Or, dans notre cas, $x = \beta - \alpha$ et comme α est un des zéros de f les plus proches de β, 0 est un des zéros de u les plus proches de $\beta - \alpha$, et il n'existe aucun zéro de u « proche » de $\beta - \alpha$ (voir mes Notes des Comptes Rendus, t. 222 (1946), pp. 37-40, 165-167, 363-365, 581-583).

lus proches d'un $\alpha \in Z(f)$,

Max $[\Delta(f, g), \Delta(f, h)]$.

$\Delta(f, g)$.

$g)$,

iel est $\Delta(f, g)$,

$i]$,

[5]). Pour un $f \in S_k$ fixé,

de Newton $\Pi^{(\alpha)}_{k/K}$ de

ente $\to \nu$, soit $\varphi^{(\alpha)}_{K/k}(\nu)$ l'ordonnée
facilement que l'expression précé-
s inégalités de Cauchy de l'Analyse
$\omega(u(x)) \geqslant \varphi^{(\alpha)}_{K/k}(\omega(x))$, mais
de u, qui soit « proche » de x,
$-\alpha$ et comme α est un des zéros
$\beta - \alpha$, et il n'existe aucun zéro
222 (1946), pp. 37-40, 165-167,

c'est une fonction strictement croissante $M_f(\Delta)$ de $\Delta = \Delta(f, g)$. Si $f(x)$ est séparable (donc $r_2 = \Delta(f) > 0$), et si $\Delta < \Delta(f)$, on a

$$M\ (\Delta) = (r_2 \ldots r_n)\,\Delta \qquad \text{donc} \quad = |\mathfrak{d}_f|\,\Delta,$$

où $\mathfrak{d}_f$ [la *différente* de $f(x)$] est l'idéal engendré par la dérivée $f'(\alpha)$ de $f(x)$ en α [il ne dépend pas du choix de α, car tous les $f'(\alpha)$ sont conjugués par rapport à k et ont une même valuation].

a étant un nombre réel > 0, organisons S_k par la distance

$$d_a(f, g) = |R(f, g)|^{a:nn'}$$

égale aussi à $|f(\beta)|^{a:n}$ et à $|g(\alpha)|^{a:n'}$, où α, β sont des zéros arbitraires des f, g. $d_a(f, g) = 0$ équivaut à $R(f, g) = 0$, c'est-à-dire, vu que $f(x)$ et $g(x)$ sont unitaires et irréductibles, à $f = g$. D'autre part, puisque $R(g, f) = R(f, g)$, on a

$$d_a(g, f) = d_a(f, g).$$

Enfin, puisque, pour un f fixé, $d_a(f, g)$ est une fonction strictement croissante $M_f(\Delta)^{a:n}$ de $\Delta = \Delta(f, g)$, et puisque, si f, g, h sont $\in S_k$, un au moins des $\Delta(g, f)$, $\Delta(h, f)$ est $\geqslant \Delta(g, h)$, un au moins des $d_a(g, f)$, $d_a(h, f)$ est $\geqslant d_a(g, h)$ et $d_a(g, h) \leqslant \mathrm{Max}\,[d_a(g, f), d_a(h, f)]$. Ainsi, $d_a(f, g)$ est une distance ultramétrique, et l'on notera $S_{k,a}$ l'ensemble S_k, organisé en espace ultramétrique par cette distance. On aura à considérer, en particulier, le sous-ensemble de S_k constitué par les $f \in S_k$ de degré n. On le considérera toujours comme un sous-espace de l'espace $S_{k,n}$ (on fera donc le choix $a = n$), et ce sous-espace sera noté $S_k^{(n)}$. Sa distance est

$$d_n(f, g) = |f(\beta)|\ [\beta \in Z(g)].$$

3° Soit T l'application $\beta \to f_{\beta/k}(x)$ de $\mathfrak{K}$ sur S_k appliquant tout $\beta \in \mathfrak{K}$ sur son polynome minimal $f_{\beta/k}(x)$ par rapport à k. Soient

$$\alpha, \beta \in \mathfrak{K}, \qquad f(x) = T.\alpha, \qquad g(x) = T.\beta.$$

Alors, on a $\Delta(f, g) \leqslant |\beta - \alpha|$, d'où, si n est le degré de $f(x)$,

$$d_n(f, g) = M_f(\Delta(f, g)) \leqslant M_f(|\beta - \alpha|).$$

Ainsi, T applique le cercle (par exemple, circonférencié) $C(\alpha, r; \mathfrak{K})$ de centre α et de rayon r dans $\mathfrak{K}$ dans le cercle $C(f, M_f(r); S_{k,n})$ de centre f et de rayon $M_f(r)$ dans $S = S_{k,n}$.

Montrons que

$$T.C(\alpha, r; \mathfrak{K}) = C(f, M_f(r); S).$$

En effet, soit $g \in C(f, M_f(r); S)$ et soit β' un zéro de g dans $\mathfrak{K}$, donc $g = T.\beta'$. Soit $\alpha' = \alpha(\beta')$ un des zéros de f les plus proches de β'. Alors, on a

$$d_n(f, g) = M_f(d(\alpha', \beta'))$$

et, puisque $M_f(r)$ est strictement croissante et $d_n(f, g) \leqslant M_f(r)$, on a $d(\alpha', \beta') \leqslant r$. Mais il existe un $\sigma \in G$ tel que $\sigma.\alpha' = \alpha$, d'où, si $\beta = \sigma.\beta'$, on a

$$d(\alpha, \beta) = d(\alpha', \beta') \leqslant r \qquad \text{et} \qquad \beta \in C(\alpha, r; \mathfrak{K}).$$

Et, β étant un zéro de g, on a

$$g = T.\beta \in T.C(\alpha, r; \mathfrak{K}).$$

Nous voyons, en plus, que tout $\beta \in T^{-1}.C(f, M_f(r); S)$ a un conjugué (par rapport à k) dans $C(\alpha, r; \mathfrak{K})$, donc appartient à un conjugué $C(\alpha_i, r; \mathfrak{K})$ de ce dernier cercle. Certains de ces cercles peuvent être confondus, mais cela n'arrive pas si $f(x)$ est séparable et $r < \Delta(f)$, auquel cas leur nombre est exactement n.

Soit $\mathfrak{K}'$ un sous-espace quelconque de $\mathfrak{K}$, stable par les automorphismes de $\mathfrak{K}/k$, et soit $S' = T.\mathfrak{K}'$. Alors, visiblement,

$$\mathfrak{K}' = T^{-1}.S', \qquad T.C(\alpha, r; \mathfrak{K}') = C(f, M_f(r); S')$$

(où $\alpha \in \mathfrak{K}'$) et $T^{-1}.C(f, M_f(r); S')$ est la réunion des $C(\alpha_i, r; \mathfrak{K}')$ $(i = 1, 2, \ldots, n)$. L'ensemble $\mathfrak{K}^{(n)}$ des $\alpha \in \mathfrak{K}$ de degré n par rapport à k est un tel sous-espace $\mathfrak{K}'$ de $\mathfrak{K}$ et $T.\mathfrak{K}^{(n)} = S_k^{(n)}$.

4° Soient $\alpha \in \mathfrak{K}$ séparable sur k et $C_\alpha = C(\alpha, \Delta(f)^-; \mathfrak{K})$ le plus grand cercle de centre α dans $\mathfrak{K}$ ne contenant aucun de ses conjugués $\alpha' \neq \alpha$ par rapport à k [c'est le cercle non circonférencié de centre α et de rayon $\Delta(f)$, où $f = T.\alpha$]. Alors, tout $\beta \in C_\alpha$ est plus près de α que de tout son conjugué $\alpha' \neq \alpha$ par rapport à k. *Il en résulte* $k(\beta) \supseteq k(\alpha)$. En effet, tout conjugué de $\alpha - \beta$ par rapport au corps (qui est complet) $k(\beta)$ est de la forme $\alpha' - \beta$, où α' est un conjugué de α par rapport à k, et, en plus, on doit avoir $|\alpha' - \beta| = |\alpha - \beta|$, ce qui implique $\alpha' = \alpha$. Par suite, $\alpha - \beta$ et, également, $\alpha = (\alpha - \beta) + \beta$ n'a d'autre conjugué par rapport à $k(\beta)$ que lui-même. Étant séparable par rapport à k, α l'est, à fortiori, par rapport à $k(\beta)$, ce qui implique $\alpha \in k(\beta)$ et $k(\beta) \supseteq k(\alpha)$. En particulier, $(k(\beta) : k)$ est $\geqslant (k(\alpha) : k)$ et l'égalité de ces degrés implique $k(\beta) = k(\alpha)$ (et la séparabilité de β par rapport à k). En plus, dans ce cas, pour toute paire σ_1 et $\sigma_2 \neq \sigma_1$ d'isomorphismes de $k(\alpha)/k$ dans $\mathfrak{H}$, $d(\sigma_1 . \beta, \sigma_1 . \alpha)$ et $d(\sigma_2 . \beta, \sigma_2 . \alpha)$ sont égaux à $d(\beta, \alpha) < \Delta(f)$, qui est $\leqslant d(\sigma_1 . \alpha, \sigma_2 . \alpha)$, d'où résulte que

$$d(\sigma_1 . \beta, \sigma_2 . \beta) = d(\sigma_1 . \alpha, \sigma_2 . \alpha).$$

Ainsi, les distances mutuelles des conjugués d'un $\beta \in C_\alpha \cap \mathfrak{K}^{(n)}$ sont les mêmes que celles des conjugués de α, d'où résulte, si $g = T . \beta$,

que
$$M_g(r) = M_f(r)$$

et, en particulier, $\mathfrak{d}_g = \mathfrak{d}_f$; d'autre part, on a, manifestement, $|\beta| = |\alpha|$.

5° K/k étant une extension séparable de degré $(K : k) = n$ fini, soient K_k l'ensemble des $\alpha \in K$ tels que $K = k(\alpha)$, $(K ; \mathfrak{d})$ celui des entiers $(|\alpha| \leqslant 1)$ $\alpha \in K$, dont la différente $\mathfrak{d}_{\alpha/k} = \mathfrak{d}_{T.\alpha}$ est $\mathfrak{d}$, $K^{(d)} = (K ; \mathfrak{d}_{K/k})$ celui des éléments discriminantiels de K/k, autrement dit celui de ses entiers, dont la différente est égale à celle de K/k (c'est-à-dire a la plus grande valuation possible). Si $|\alpha| < 1$, les $d(\alpha, \sigma . \alpha)$ sont < 1, d'où, si $f = T . \alpha$, $|\mathfrak{d}_f| = |f'(\alpha)|$ est $\leqslant \Delta(f)$. Si $\alpha \in (K ; \mathfrak{d})$ et si $\beta \in C_\alpha \cap \mathfrak{K}^{(n)}$, on a

$$k(\beta) = k(\alpha), \quad |\beta| = |\alpha| \leqslant 1 \qquad \text{et} \qquad \mathfrak{d}_{\beta/k} = \mathfrak{d}_{\alpha/k} = \mathfrak{d},$$

donc $\beta \in (K ; \mathfrak{d})$. Or, $d(\beta, \alpha) < |\mathfrak{d}| = |\mathfrak{d}_f|$ implique $d(\beta, \alpha) < \Delta(f)$, donc $\beta \in C_\sigma$. Donc, si $r < |\mathfrak{d}|$, $(K ; \mathfrak{d})$ (et, en particulier, $K^{(d)}$ si $\mathfrak{d} = \mathfrak{d}_{K/k}$) est une réunion de cercles de rayon r dans $\mathfrak{K}^{(n)}$, et il en est de même pour les ensembles $(K ; \mathfrak{d})_w$, $(K^{(d)})_w$ des $\alpha \in (K ; \mathfrak{d})$ respectivement $\in K^{(d)}$ tels que $|\alpha| = w$, ainsi que pour les réunions arbitraires de tels ensembles avec $\mathfrak{d}$ fixé. Ainsi, si Λ est une famille d'extensions $K \subset \mathfrak{K}$ de k de degré n, les réunions $L_{\Lambda, \mathfrak{d}}$ et $(L_{\Lambda, \mathfrak{d}})_w$ des $(K ; \mathfrak{d})$ respectivement $(K ; \mathfrak{d})_w$, où K parcourt Λ, se décomposent, pour $r < |\mathfrak{d}|$, en réunion de cercles de rayon r dans $\mathfrak{K}^{(n)}$. Si toutes les $K/k \in \Lambda$ ont une même différente $\mathfrak{d}$, il en est de même pour

$$L_\Lambda^{(d)} = L_{\Lambda, \mathfrak{d}} \qquad \text{et} \qquad (L_\Lambda^{(d)})_w = (L_{\Lambda, \mathfrak{d}})_w.$$

Si k est discrètement valué, $K^{(d)} \neq \emptyset$; si, en plus, K/k est complètement étagé (c'est-à-dire son degré résiduel est 1), $|\alpha| = |\mathfrak{P}| = |\mathfrak{p}|^{1 : n}$

implique que α est discriminantiel, donc $(\mathrm{K}^{(d)})_w$, où $w = |\mathfrak{P}| = |\mathfrak{p}|^{1:n}$ coïncide avec le complément Π_K de $\mathfrak{P}^2$ dans $\mathfrak{P}$. Si $\Lambda = \Lambda_{n,j}^{(r)}$ est la famille de toutes les extensions $\mathrm{K} \subset \mathfrak{K}$ de k complètement étagées de degré n et de différente $\mathfrak{d} = \mathfrak{p}\mathfrak{P}^{j-1}$, $(\mathrm{L}_{\Lambda,\mathfrak{d}})_w$ est la réunion des Π_K, étendue aux $\mathrm{K} \in \Lambda_{n,j}^{(r)}$, qui sera également notée $\Pi_{k,n,j}$ et se décompose en réunion de cercles de rayon $r = |\mathfrak{P}|^t$, pourvu que $t \geqslant n + j$.

Si $(\mathrm{K} : k) = n$, l'ensemble $\mathrm{S}_{\mathrm{K}/k}$ des $f \in \mathrm{S}_k$ définissant K/k et ceux $(\mathrm{S}_{\mathrm{K}/k}; \mathfrak{d})$, $(\mathrm{S}_{\mathrm{K}/k}; \mathfrak{d})_\mathrm{W}$, $\mathrm{S}_{\mathrm{K}/k}^{(d)}$, et $(\mathrm{S}_{\mathrm{K}/k}^{(d)})_\mathrm{W}$ des $f \in \mathrm{S}_{\mathrm{K}/k}$ à coefficients entiers et tels que respectivement $\mathfrak{d}_f = \mathfrak{d}$, $\mathfrak{d}_f = \mathfrak{d}$ et la valuation du terme constant $c(f)$ de f est $|c(f)| = \mathrm{W}$, $\mathfrak{d}_f = \mathfrak{d}_{\mathrm{K}/k}$, $\mathfrak{d}_f = \mathfrak{d}_{\mathrm{K}/k}$ et $|c(f)| = \mathrm{W}$, sont des sous-espaces de $\mathrm{S}_k^{(n)}$. On a

$$\mathrm{T}.\mathrm{K}_k = \mathrm{S}_{\mathrm{K}/k}, \qquad \mathrm{T}.(\mathrm{K}; \mathfrak{d}) = (\mathrm{S}_{\mathrm{K}/k}; \mathfrak{d}), \qquad \mathrm{T}.(\mathrm{K}; \mathfrak{d})_w = (\mathrm{S}_{\mathrm{K}/k}; \mathfrak{d})_{w^n},$$

et, en particulier,

$$\mathrm{T}.\mathrm{K}^{(d)} = \mathrm{S}_{\mathrm{K}/k}^{(d)} \qquad \text{et} \qquad \mathrm{T}.(\mathrm{K}^{(d)})_w = (\mathrm{S}_{\mathrm{K}/k}^{(d)})_{w^n}.$$

Les propriétés prouvées de T impliquent que $\mathfrak{d}_f = \mathfrak{d}$ et $r < |\mathfrak{d}|$ (donc aussi $r < \Delta(f)$) quand les coefficients de f sont entiers entraînent $\mathrm{M}_f(r) = |\mathfrak{d}|\, r$ et, si $f(\alpha) = 0$, $\quad \mathrm{T}.\mathrm{C}(\alpha, r; \mathfrak{K}^{(n)}) = \mathrm{C}(f, |\mathfrak{d}|\, r; \mathrm{S}_k^{(n)})$.

Ainsi, si $r < |\mathfrak{d}|$, $(\mathrm{S}_{\mathrm{K}/k}; \mathfrak{d})$ et $(\mathrm{S}_{\mathrm{K}/k}; \mathfrak{d})_\mathrm{W}$ sont des réunions de cercles de rayon $|\mathfrak{d}|\, r$ dans $\mathrm{S}_k^{(n)}$; il en est de même pour

$$\mathrm{L}_{\Lambda,\mathfrak{d}} = \bigcup (\mathrm{S}_{\mathrm{K}/k}; \mathfrak{d}) \qquad \text{et} \qquad (\mathrm{L}_{\Lambda,\mathfrak{d}})_\mathrm{W} = \bigcup (\mathrm{S}_{\mathrm{K}/k}; \mathfrak{d})_\mathrm{W},$$

où la réunion est étendue aux $\mathrm{K} \in \Lambda$. En particulier, si k est discrètement valué, on voit (en posant $\Lambda = \Lambda_{n,j}^{(r)}$ et $\mathrm{W} = |\mathfrak{p}|$) que $\mathrm{T}.\Pi_{k,n,j}$ se décompose en cercles de rayon $|\mathfrak{d}|\, r = |\mathfrak{P}|^{n+j-1+t}$ dès que $t \geqslant n + j$. Or, $f \in \mathrm{S}_k^{(n)}$ définit un élément α d'une extension complètement étagée K/k tel que $|\alpha| = |\mathfrak{P}|$ si, et seulement si $|c(f)| = |\mathfrak{p}|$, autrement dit f est un polynôme d'Eisenstein. Ainsi, $\mathrm{T}.\Pi_{k,n,j}$ est l'ensemble $\mathrm{E}_{k,j}^{(n)}$ des polynômes d'Eisenstein $f(x) \in k[x]$ de degré n et de différente $\mathfrak{p}\mathfrak{P}^{j-1} = \mathfrak{p}^{(n+j-1):n}$.

Soit $\mathrm{C}' \subseteq \mathrm{E}_{k,j}^{(n)}$ un cercle de rayon $|\mathfrak{d}|\, r = |\mathfrak{p}|\, |\mathfrak{P}|^{j-1+t}$ dans $\mathrm{S}_k^{(n)}$, et soit K/k une extension (complètement étagée) définie par les $f \in \mathrm{C}'$. Alors, $\mathrm{T}^{-1}.\mathrm{C}'$ est la réunion de n cercles disjoints $\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_n$ de rayon $r = |\mathfrak{P}|^t$ dans $\mathfrak{K}^{(n)}$. Si $l = l_{\mathrm{K}/k}$ est le nombre des extensions $\mathrm{K}' \subset \mathfrak{K}$ de k conjugués de K/k, chaque cercle C_i est contenu dans quelque K' de cette sorte et dans un seul, et le nombre des $\mathrm{C}_i \subseteq \mathrm{K}'$ ne dépend pas du choix de K'. Ainsi, $\mathrm{T}^{-1}.\mathrm{C}' \cap \mathrm{K}$ est la réunion de $n : l$ cercles de rayon r dans $\mathfrak{K}^{(n)}$.

6° Supposons que k est localement compact (autrement dit discrètement valué et à corps résiduel fini, dont soit $q = p^{f_0}$ le nombre d'éléments). Soit K/k une extension complètement ramifiée (donc, $\bar{k}$ étant parfait, complètement étagée). Les cercles de rayon $r = |\mathfrak{P}|^t$ dans K sont des classes (mod $\mathfrak{P}^t$) dans ce corps. Comme les corps résiduels de K et de k coïncident, chaque classe (mod $\mathfrak{P}^i$) contient q classes (mod $\mathfrak{P}^{i+1}$), et Π_K se décompose en $q^{t-1} - q^{t-2}$ classes (mod $\mathfrak{P}^t$), c'est-à-dire des cercles de rayon $r = |\mathfrak{P}|^t$. Si $E_{K/k}$ est l'ensemble des polynomes d'Eisenstein définissant K/k, on a $\Pi_K = T^{-1}.E_{K/k} \cap K$. $E_{K/k}$ est une réunion de cercles C' de $S_k^{(n)}$ de rayon $|\mathfrak{d}_{K/k}|\, r$, où $r = |\mathfrak{P}|^t$ est $< |\mathfrak{d}_{K/k}|$, et $T^{-1}.C' \cap K$ est la réunion de $n : l_{K/k}$ cercles de rayon r. Par suite, comme Π_K contient $(q-1)\, q^{t-2}$ tels cercles, $E_{K/k}$ est la réunion de $n^{-1}(q-1)\, q^{t-2}\, l_{K/k}$ cercles disjoints C' de rayon $|\mathfrak{d}_{K/k}|\, r$.

Partageons $\Lambda_{n,j}^{(r)}$ en classes des corps conjugués par rapport à k. Alors, les ensembles $E_{K/k} = T.\Pi_K$ coïncident ou sont disjoints selon que les corps K correspondants appartiennent à une même classe L, et si $l(L)$ désigne le nombre des corps $\in L$, le nombre des cercles de rayon $|\mathfrak{d}|\, r = |\mathfrak{p}|\, |\mathfrak{P}|^{j+t-1}$ constituant $E_{K/k}$, où $K \in L$, est $n^{-1}(q-1)\, q^{t-2}\, l(L)$. Par suite, le nombre $N_{k,j,t}^{(n)}$ des cercles de rayon $|\mathfrak{p}|^{(n+j+t-1):n}$ constituant $E_{k,j}^{(n)} = \cup\, E_{K/k}$ $(K \in \Lambda_{n,j}^{(r)})$ est $n^{-1}(q-1)\, q^{t-2} \sum l(L)$, où L parcourt toutes les classes de $\Lambda_{n,j}^{(r)}$. Or, une telle somme $\sum l(L)$ est, visiblement, le nombre $\mathfrak{N}_{k,n,j}^{(r)}$ des extensions complètement ramifiées $K \subset \mathfrak{K}$ de k telles que $(K : k) = n$ et $\mathfrak{d}_{K/k} = \mathfrak{p}\, \mathfrak{P}^{j-1}$. D'où résulte

$$\mathfrak{N}_{k,n,j}^{(r)} = n N_{k,j,t}^{(n)} : (q-1)\, q^{t-2}.$$

Il suffit donc de prouver que $N_{k,j,t}^{(r)}$ est fini et de le calculer pour démontrer que $\mathfrak{N}_{k,n,j}^{(r)}$ l'est, et déterminer sa valeur.

7° On va normaliser la valuation de k en posant $|\mathfrak{p}| = e^{-n}$, donc $\omega(\mathfrak{p}) = n$. Alors, si $\mathfrak{P}$ est l'idéal premier d'une extension complètement ramifiée $K \subset \mathfrak{K}$ de k de degré n, on a $\omega(\mathfrak{P}) = 1$, et si $\mathfrak{d} = \mathfrak{p}\mathfrak{P}^{j-1}$, on a

$$\omega(\mathfrak{d}) = n + j - 1.$$

On a

$$r = |\mathfrak{P}|^t = e^{-t} \qquad \text{et} \qquad |\mathfrak{d}|\, r = e^{-(n+j-1+t)}.$$

Si

$$f(x) = a_0 + a_1 x + \dots + a_i x^i + \dots + a_n x^n \qquad \text{est} \qquad \in k[x],$$

$a_i \neq 0$ implique $\omega(a_i) \equiv 0 \pmod{n}$. $f(x)$, supposé unitaire, est un polynome d'Eisenstein si, et seulement si $\omega(a_0) = n$ et $\omega(a_i) \geqslant n$ pour tout i tel que $0 < i < n$. Si α est un zéro dans k d'un polynome d'Eisenstein $f(x)$ de degré n, on a $\omega(\alpha) = 1$.

Ceci posé, soient

$$f(x) = x^n + \sum a_i x^i \qquad \text{et} \qquad g(x) = x^n + \sum b_i x^i$$
$$(i = 0, 1, \ldots, n-1)$$

deux polynomes d'Eisenstein dans k, α un zéro de f dans k, et β celui de g. Alors,

$$f(\beta) = f(\beta) - g(\beta) = \sum (a_i - b_i) \beta^i \qquad (i = 0, 1, \ldots, n-1).$$

Or, on a

$$\omega((a_i - b_i)\beta^i) = \omega(a_i - b_i) + i\,\omega(\beta),$$
$$\omega(\beta) = 1 \qquad \text{et} \qquad \omega(a_i - b_i) \equiv 0 \qquad (\mathrm{mod}\ n),$$

d'où

$$\omega((a_i - b_i)\beta^i) \equiv i \qquad (\mathrm{mod}\ n).$$

Ainsi tous les termes de la somme précédente ont leurs ordres (et valuations) différents et $|f(\beta)| = |f(\beta) - g(\beta)|$ est $\mathrm{Max}(|a_i - b_i|\,|\beta|^i)$ $(i = 0, 1, \ldots, n-1)$. Par suite, $d(f, g) = d_n(f, g)$ est l'exponentielle de $-\mathrm{Min}[\omega(a_i - b_i) + i]$ $(i = 0, 1, \ldots, n-1)$. Il est à remarquer $d(f, g)$ est encore $\mathrm{Max}(|a_i - b_i|\,|\pi|^i)$, où π est un élément arbitraire de $\mathfrak{K}$ tel que $\omega(\pi) = 1$.

On a

$$|\mathfrak{d}_f| = |f'(\alpha)| = \left| n\,\alpha^{n-1} + \sum i a_i\,\alpha^{i-1} \right| \qquad (i = 1, \ldots, n-1).$$

Or, n et ia_i sont $\in k$, donc $\omega(n)$ et $\omega(ia_i)$ sont $\equiv 0 \pmod{n}$. Par suite, quand les termes en question ne sont pas nuls,

$$\omega(n\,\alpha^{n-1}) \equiv n - 1 \quad (\mathrm{mod}\ n) \qquad \text{et} \qquad \omega(ia_i\,\alpha^{i-1}) \equiv i - 1 \quad (\mathrm{mod}\ n).$$

Ainsi, tous ces termes ont des ordres différents ou $= +\infty$ et

$$\omega(\mathfrak{d}_f) = \mathrm{Min}\Big[\omega(n) + n - 1, \qquad \mathrm{Min}_i[\omega(i) + \omega(a_i) + i - 1]\Big].$$

Soient

$$n = hp^m, \qquad (p) = \mathfrak{P}^{E} = \mathfrak{p}^{E/n}$$

et $p^{s(i)}$ la contribution de p dans i. Alors $\omega(\mathfrak{d}_j)$ est

$$\mathrm{Min}\left[m\mathrm{E} + n - 1, \qquad \mathrm{Min}_i\,[s(i)\mathrm{E} + \omega(a_i) + i - 1]\right].$$

Or $f \in \mathrm{E}_{k,j}^{(n)}$ équivaut à $\omega(\mathfrak{d}_f) = n + j - 1$, ce qui peut s'écrire

$$\mathrm{Min}\left[m\mathrm{E}, \qquad \mathrm{Min}_i\left[s(i)\mathrm{E} + [\omega(a_i) - n] + i\right]\right] = j,$$

d'où résulte $j \leqslant m\mathrm{E}$. Si le terme maximal de $f'(\alpha)$ est $n\alpha^{n-1}$, on a $j = m\mathrm{E}$. Si c'est un terme $i^* a_{i^*} \alpha^{i^*-1}$, on doit d'abord avoir

$$s(i^*)\mathrm{E} + \omega(a_{i^*}) - n + i^* < m\mathrm{E},$$

et, vu que $\omega(a_{i^*}) \geqslant n$ pour tout $i = 1, 2, \ldots, n-1$, et que $i^* > 0$, ceci entraîne $s(i^*) < m$. D'autre part,

$$s(i^*)\mathrm{E} + \omega(a_{i^*}) - n + i^* = j \qquad \text{implique } j \equiv i^* \pmod{n}$$

[et, plus précisément, puisque $0 < i^* < n$, que i^* est le plus petit reste positif de $j \pmod{n}$], d'où puisque $p^m | n$, $s(j) = s(i^*)$. Mais $\omega(a_{i^*}) \geqslant n$ et $i^* > 0$ entraînent alors $j > s(i^*)\mathrm{E}$, donc $>$ et à fortiori, $\geqslant s(j)\mathrm{E}$. Ainsi si s est le plus grand entier $< m$ tel que $p^s | j$, et si $\mathfrak{d}_f = \mathfrak{p}\mathfrak{P}^{j-1}$, on doit avoir $s\mathrm{E} \leqslant j \leqslant m\mathrm{E}$ (conditions d'Ore [*10*]). Inversement, si j satisfait à ces conditions, il existe un $f \in \mathrm{E}_{k,j}^{(n)}$. En effet, pour $j = m\mathrm{E}$ (ce qui implique que k est $\mathfrak{p}$-adique), tel est le polynome $x^n - a_0$, où $a_0 \in k$ et $\omega(a_0) = n$, car sa différente est $(n\,\alpha^{n-1}) = \mathfrak{P}^{m\mathrm{E}-1}$. Et si $j < m\mathrm{E}$ et $\not\equiv 0 \pmod{p^m}$ est $\geqslant$ (donc $>$) que $s(j)\mathrm{E}$, soit i^* le plus petit reste positif de $j \pmod{n}$. Alors le polynome $x^n + a_{i^*} x^{i^*} + a_0$, où $a_0, a_{i^*} \in k$ sont tels que $\omega(a_0) = n$ et $\omega(a_{i^*}) - n = (j - i^*) - s(j)\mathrm{E}$ [ce dernier entier est $\geqslant 0$ et divisible par n] est $\in \mathrm{E}_{k,j}^{(n)}$. Ainsi $\mathrm{E}_{k,j}^{(n)} \neq \emptyset$ si, et seulement si j satisfait aux conditions d'Ore.

8º Soit L un corps discrètement valué complet, $\mathfrak{y}$ l'idéal premier de son anneau d'intégrité, $\varkappa$ un élément de L tel que $\mathfrak{y} = (\varkappa)$, $\overline{\mathrm{L}}$ le corps résiduel de L, p la caractéristique de $\overline{\mathrm{L}}$, $\lambda : \overline{\mathrm{L}} \to \mathrm{L}$ une fonction représentative normée de $\overline{\mathrm{L}}$ dans L, c'est-à-dire une application de $\overline{\mathrm{L}}$ dans L telle que, pour tout $\bar{c} \in \overline{\mathrm{L}}$, $\lambda.\bar{c}$ (dit le représentant de $\bar{c}$) soit $\in \bar{c}$ [considéré comme un sous ensemble de L] et que le représentant $\lambda.\bar{0}$ du 0 de $\bar{L}$ soit celui 0 de L. On sait que tout $\alpha \in L$ peut se représenter (et d'une manière unique) comme la somme d'une série $\sum [\lambda.\bar{c}_t(\alpha)]\varkappa^t$, où la sommation est étendue à l'ensemble $\mathbf{Z}$ de tous les entiers rationnels, mais où $c_t(\alpha) = \bar{0}$ si t est inférieur à une constante convenable. Plus précisément, le plus petit t tel que $\bar{c}_t(\alpha) \neq \bar{0}$, qui existe si $\alpha \neq 0$ est $\omega(\alpha)/\omega(\mathfrak{y})$. Et la distance $d(\alpha, \beta) = |\alpha - \beta|$ des $\alpha, \beta \in L$ est $|\mathfrak{y}|^t$ où t est le plus petit indice tel que $\bar{c}_t(\alpha) \neq \bar{c}_t(\beta)$. Le développement précédent de α sera dit son $(\lambda, \varkappa)$-développement.

Soit $\varphi(\alpha)$ le vecteur de $\bar{L}^{\mathbf{Z}}$ dont la $t^{\text{ième}}$ coordonnée $\varphi(\alpha)_t$ soit, pour tout $t \in \mathbf{Z}$, $\bar{c}_t(\alpha)$, et soit $\varphi(\lambda, \varkappa)$ l'application $\alpha \to \varphi(\alpha)$. Alors $\varphi(\lambda, \varkappa)$. L est l'ensemble $\mathfrak{Y}(\bar{L})$ des vecteurs $\varphi = (\varphi_t)$ de $\bar{L}^{\mathbf{Z}}$, dont les coordonnées φ_t sont nulles quand t est inférieur à une constante convenable; et l'image par $\varphi(\lambda, \varkappa)$ de l'anneau d'intégrité I (L) de L est l'ensemble de tels vecturs dont les coordonnées d'indices négatifs sont nulles, cet ensemble s'identifiant, d'une manière évidente, avec $\bar{L}^{\mathbf{N}}$, où $\mathbf{N}$ est l'ensemble des entiers non négatifs. Si l'on organise $\mathfrak{Y}(\bar{L})$ en groupe additif valué en posant

$$|\varphi| = |\mathfrak{y}|^{-\omega(\varphi)} \qquad \text{et} \qquad d(\varphi', \varphi'') = |\mathfrak{y}|^{-\omega(\varphi', \varphi'')},$$

où $\omega(\varphi)$ est le plus petit t tel que $\varphi_t \neq \bar{0}$ et $\omega(\varphi', \varphi'')$ est le plus petit t tel que $\varphi'_t \neq \varphi''_t$, $\varphi(\lambda, \varkappa)$ devient une isométrie de L sur $\mathfrak{Y}(\bar{L})$, préservant, en particulier, la valuation. Si C est un cercle de L de rayon $r = |\mathfrak{y}|^{t_0}$ et si $\alpha \in C$, C est l'ensemble des $\beta \in L$ tels que $\bar{c}_t(\beta) = \bar{c}_t(\alpha)$ pour tout $t < t_0$. Donc, $\varphi(\lambda, \varkappa).C$ est l'ensemble des $\varphi \in \mathfrak{Y}(\bar{L})$ tels que $\varphi_t = \varphi(\alpha)_t$ quand $t < t_0$ et les cercles $\varphi(\lambda, \varkappa).C \subseteq \varphi(\lambda, \varkappa).I(L)$ peuvent s'identifier avec les vecteurs $(\varphi_0, \varphi_1, \ldots, \varphi_{t_0-1})$ de l'espace $\bar{L}^{t_0}$.

Si $\alpha \in L$, posons $\Delta_{\lambda,\varkappa}.\alpha = \sum t[\lambda.\bar{c}_t(\alpha)]\varkappa^{t-1}$. Montrons que si $\omega(p)/\omega(\alpha)$ est un entier (pouvant être $+\infty$), cette somme a un seul terme maximal. En effet, si $n = \omega[\varphi(\alpha)]$ est le plus petit t tel que $\bar{c}_t(\alpha) \neq \bar{0}$ et si $n = hp^m$, où $h \not\equiv 0 \pmod{p}$,

$$\left|t[\lambda.c_t(\alpha)]\varkappa^{t-1}\right| \geqslant \left|n[\lambda.c_n(\alpha)]\varkappa^{n-1}\right|$$

entraîne $t = n$ ou $t \not\equiv 0 \pmod{p^m}$. Ainsi, si $n[\lambda.\bar{c}_n(\alpha)]\varkappa^{n-1}$ est maximal, c'est le terme maximal unique. Et, s'il ne l'est pas et $t'[\lambda.\bar{c}_{t'}(\alpha)]\varkappa^{t'-1}$ et $t''[\lambda.\bar{c}^{t''}(\alpha)]\varkappa^{t''-1}$ le sont, on a, puisque $t' - t'' = [\omega(t'') - \omega(t')]$: $\omega(\varkappa) \equiv 0 \; (\operatorname{mod} \omega(p)/\omega(\varkappa))$ et, à fortiori, $(\operatorname{mod} \omega(\alpha)/\omega(\varkappa) = n = hp^m)$, que la contribution de p dans t' et t'', et par suite, leur valuation est la même, ce qui implique $t' = t''$ [car $|t'| = |t''|$, $|\lambda.\bar{c}_t(\alpha)| = 1$ quand $\bar{c}_t(\alpha) \neq 0$ et l'égalité des valuations des termes considérés entraînent $|\varkappa|^{t'-1} = |\varkappa|^{t''-1}$]. Donc, si $\Delta_{\lambda,\varkappa}.\alpha \neq 0$, $\omega(\Delta_{\lambda,\varkappa}.\alpha)$ est le minimum des ordres des termes non nuls de la série précédente, donc

$$\mathrm{Min}\,[s(t)\,\omega(p) + (t-1)\,\omega(\varkappa)],$$

où la somme est étendue aux $t \geqslant n$ tels que $c_t(\alpha) \neq 0$. Si $\mathrm{E} = \omega(p)/\omega(\mathfrak{y})$, ceci peut s'écrire $\mathrm{Min}\,[s(t)\,\mathrm{E} + t - 1]\,\omega(\mathfrak{y})$.

9° Soient $k[x]_n$ l'ensemble des polynômes unitaires

$$f(x) = x^n + \sum a_i\, x^i \qquad (0 \leqslant i < n)$$

de degré n dans k, π_0 un élément de k tel que $\mathfrak{p} = (\pi_0)$, $\lambda : \bar{k} \to k$ une fonction représentative normée de $\bar{k}$ dans k, $a_i = \sum (\lambda.\bar{a}_{i,u})\,\pi_0^u$ le (λ, π_0)-développement de a_i. Soient

$$\varkappa = \sqrt[n]{\pi_0} \qquad \text{et} \qquad \mathrm{L} = k(\varkappa)$$

organisé par l'unique prolongement possible de la valuation de k. L/k est une extension complètement ramifiée, dont $\mathfrak{y} = (\varkappa) = (\pi_0^{1/n})$ est l'idéal premier, et l'on a avec la normalisation du paragraphe 6,

$$\omega(\mathfrak{y}) = n^{-1}\,\omega(\pi_0) = 1.$$

Soit θ l'application

$$f(x) \quad\to\quad f(\varkappa) - \varkappa^n = \sum a_i\,\varkappa^i \quad \text{de} \quad k[x]_n$$

dans L. C'est une surjection car $(a_0, a_1, \ldots, a_{n-1})$ est un vecteur arbitraire de k^n et $(1, \varkappa, \ldots, \varkappa^{n-1})$ est une base linéaire de L/k. On a

$$\omega(\theta.f(x)) = \mathrm{Min}\,[\omega(a_i) + i],$$

et, par suite, les conditions :

$$\omega(a_0) = n, \qquad \omega(a_i) \geqslant n \qquad (0 < i < n),$$

qui caractérisent les polynômes d'Eisenstein, équivalent à $\omega(\theta . f(x)) = n$. Et si

$$g(x) = x^n + \sum b_i x^i \qquad \text{est} \qquad \in k[x]_n,$$

$$d(\theta . f(x), \theta . g(x)) \qquad \text{est} \qquad |f(x) - g(x)| = \left| \sum (a_i - b_i) \varkappa^i \right|,$$

ce qui coïncide, en vertu du paragraphe 6, avec la distance $d_n(f(x), g(x))$ des $f(x)$, $g(x)$ dans $S_k^{(n)}$. Ainsi, $\theta . E_{k,n}$ (où $E_{k,n}$ est l'ensemble des polynômes d'Eisenstein de degré n dans k) est le complément $\mathfrak{p}^n \cdot\cdot \mathfrak{p}^{n+1}$ de $\mathfrak{p}^{n+1}$ dans $\mathfrak{p}^n$ et θ est une isométrie du sous-espace $E_{k,n}$ de $S_{k,n}$ dans L. Comme λ est aussi une fonction représentative normée de $\overline{L} = \overline{k}$ dans L, $\varphi(\lambda, \varkappa)\,\theta$ est une isométrie de $E_{k,n}$ dans $(\overline{L}^{\mathbf{Z}})$. Puisque $\pi_0 = \varkappa^n$, on a

$$\theta . f(x) = \sum_i a_i \varkappa^i = \sum_i \left(\sum_u (\lambda . \overline{a}_{i,u}) \pi_0^u \right) \varkappa^i = \sum_i \sum_u (\lambda . \overline{a}_{i,u}) \varkappa^{nu+i}$$

et, si $N_n = \{0, 1, \ldots, n-1\}$, $(u, i) \to nu + i$ est une bijection de $\mathbf{Z} \times \mathbf{N}_n$ sur $\mathbf{Z}$, un $t \in \mathbf{Z}$ étant l'image du couple $[u(t), i(t)]$, où $i(t)$ et $u(t)$ sont le plus petit reste non négatif de $t \pmod{n}$ et la partie entière de t/n. Ainsi si l'on pose $\overline{c}_t = \overline{a}_{i(t),u(t)}$, $\sum_t (\lambda . \overline{c}_t) \varkappa^t$ est le $(\lambda, \varkappa)$-développement de $\theta . f(x)$ et $\varphi(\lambda, \varkappa)\,\theta . f(x)$ est le vecteur $\overline{c} = (c_t = \overline{a}_{i(t),u(t)})$. Quand $f(x)$ parcourt $E_{k,n}$, ce vecteur parcourt tous les vecteurs $\overline{c} = (\overline{c}_t)\,k$ tels que $\overline{c}_t = 0$ si $t < n$ et $\overline{c}_n \neq \overline{0}$. Posons

$$\mathbf{N}'_n = \mathbf{N}_n \cdot\cdot \{0\} = \{1, \ldots, n-1\}.$$

Si $f \in E_{k,n}$, $\omega(\mathfrak{d}_f)$ est $\mathrm{Min}\left[m\,E + n - 1, \mathrm{Min}_i\,[\omega(a_i) + s(i)\,E + i - 1]\right]$ (où i parcourt $\mathbf{N}'_n$), car $\omega(\mathfrak{p}) = 1$ dans notre cas. Or si u_i est $+\infty$ ou le plus petit u tel que $\overline{a}_{i,u} \neq \overline{0}$ selon que $a_i =$ ou $\neq 0$ $(i \in \mathbf{N}'_u)$, on a $\omega(a_i) = nu_i$ et $f \in E_{k,n}$ implique $u_0 = 1$. Comme $s(n) = m$, $mE + n - 1$ est $(nu_0 + 0) + s(nu_0 + 0)\,E - 1$, tandis que $0 < i < n$ et $\omega(a_i) \geqslant n$ implique, quand $\omega(a_i) + s(i)\,E + i - 1 \leqslant m\,E + n - 1$, $s(i) < m$ [ce qui entraîne pour tout $t \equiv i \pmod{n}$, $s(t) = s(i)$], d'où

$$\omega(a_i) + s(i)\,E + i - 1 = (nu_i + i) + s(nu_i + i)\,E - 1,$$

cette égalité restant exacte pour tout $i \in \mathbf{N}'_n$ tel que $s(i) < m$. Puisque pour $i \in \mathbf{N}'_n$ tel que $s(i) \geqslant m$, on a aussi $s(nu_i + i) \geqslant m$, on voit que

$$(nu_i + i) + s(nu_i + i)\,E - 1 > mE + n - 1.$$

quivalent à $\omega(\theta . f(x)) = n$.

$\in k[x]_n$,

$) | = \left| \sum (a_i - b_i) \varkappa^i \right|$,

c la distance $d_n(f(x), g(x))$
$_{k,n}$ est l'ensemble des poly-
e complément $\mathfrak{p}^n .. \mathfrak{p}^{n+1}$ de
espace $E_{k,n}$ de $S_{k,n}$ dans L.
e normée de $\bar{L} = \bar{k}$ dans L,
Z). Puisque $\pi_0 = \varkappa^n$, on a

$= \sum_i \sum_u (\lambda . \bar{a}_{i,u}) \varkappa^{nu+i}$

$+ i$ est une bijection de
le $[u(t), i(t)]$, où $i(t)$ et $u(t)$
) et la partie entière de t/n.
est le $(\lambda, \varkappa)$-développement

$(c_t = \bar{a}_{i(t),u(t)})$. Quand $f(x)$
vecteurs $\bar{c} = (\bar{c}_t)\, k$ tels que

$n - 1 \}$.

$[\omega(a_i) + s(i) E + i - 1]]$
as. Or si u_i est $+\infty$ ou le
$=$ ou $\neq 0$ $(i \in \mathbf{N}'_u)$, on a
me $s(n) = m$, $mE + n - 1$
te $0 < i < n$ et $\omega(a_i) \geqslant n$
$E + n - 1$, $s(i) < m$ [ce
$s(i)]$, d'où

$s(nu_i + i) E - 1$,

tel que $s(i) < m$. Puisque
$nu_i + i) \geqslant m$, on voit que

$mE + n - 1$.

Donc $\omega(\mathfrak{d}_j)$ est aussi $= \mathrm{Min}\,[(nu_i + i) + s(nu_i + i)\,E - 1]$, où i parcourt N_n. Or soit t un indice tel que $\bar{c}_t \neq 0$. Alors si $s(t) < m$, on a

$$s(t) = s[i(t)] \qquad \text{et} \qquad u(t) \geqslant u_{i(t)},$$

d'où $$t + s(t)\,E - 1 \geqslant (nu_{i(t)} + s\,[nu_{i(t)} + i(t)]\,E - 1.$$

Comme tout $(nu_i + i) + s(nu_i + i) - 1$ est, quand il est $< +\infty$, parmi les $s(t)\,E + t - 1$ tels que $\bar{c}_t \neq \bar{0}$, on voit que $\omega(\mathfrak{d}_j)$ est aussi $\mathrm{Min}\,[s(t)\,E + t - 1]$, où t parcourt les indices $\in \mathbf{Z}$ tels que $\bar{c}_t \neq \bar{0}$, donc est $= \omega\,[\Delta_{\lambda,\varkappa}\,\theta . f(x)]$.

Dès lors si $f(x) \in E_{k,n}$ (autrement dit $\bar{c}_t \neq \bar{0}$ implique $t \geqslant n$ et $t = n$ implique $\bar{c}_t \neq \bar{0}$) et si j satisfait aux conditions d'Ore, on a $\omega(\mathfrak{d}_j) = \mathfrak{p}\,\mathfrak{P}^{j-1}$ si, et seulement si $\bar{c}_t \neq \bar{0}$ implique

$$s(t)\,E + t - 1 \geqslant n - 1 + j$$

et $s(t)\,E + t - 1 = n - 1 + j$ implique $\bar{c}_t \neq \bar{0}$. Or si t satisfait à cette égalité, $s(t)$ est $< m$ ou $t = n$, donc $s(t) = m$, autrement dit $s(t) \leqslant m$. Mais, la même égalité implique $j \equiv t \pmod n$, donc $(\bmod\ p^m)$, d'où il résulte que

$$s = \mathrm{Min}\,[s(j), m] = \mathrm{Min}\,[s(t), m] = s(t).$$

Ainsi, on a $f \in E_{k,j}^{(n)}$ si, et seulement si :

1° $\bar{c}_t \neq \bar{0}$ implique $t^* = t - n \geqslant \mathrm{Max}\,[j - s(t)\,E, 0]$;

2° $t^* = 0$ ou $t^* = j - sE$ implique $\bar{c}_t \neq \bar{0}$.

Si ρ est la partie entière $[j : E]$ de $j : E$, les conditions d'Ore peuvent s'écrire

$$0 \leqslant s \leqslant \rho \leqslant m.$$

10° Supposant que c est un entier assez grand pour que $E_{k,j}^{(n)}$ se décompose en cercles de rayon $\mathfrak{P}^{n+c} = \mathfrak{p}^{n+c/n}$, calculons le nombre de ces cercles, égal, puisque $\varphi(\lambda, \varkappa)$ est une isométrie, à celui des cercles de même rayon dans $\varphi(\lambda, \varkappa)\,\theta . E_{k,j}^{(n)}$. Or puisque $f \in E_{k,n}$ implique $\bar{c}_t = 0$ quand $t^* < 0$, $\varphi(\lambda, \varkappa)\,\theta . E_{k,j}^{(n)}$ s'identifie, d'une manière évidente, à l'ensemble des vecteurs $\bar{k}^{\mathbf{N}}$ (où $\mathbf{N}$ est l'ensemble des entiers $\geqslant 0$), dont les composantes $\bar{c}_t$, $t \in \mathbf{N}$, satisfont aux conditions 1°) et 2°) précédentes, et l'ensemble des cercles de rayon $\mathfrak{P}^{n+c}$, en lesquels il se décompose, s'identifie avec sa projection dans $\bar{k}^{\mathbf{N}_{n+c}}$, c'est-à-dire avec l'ensemble $\mathrm{V}_{k,j}^{(n,c)}$ des vecteurs $\bar{\varphi} = (\bar{\varphi}_0, \bar{\varphi}_1, \ldots, \bar{\varphi}_{n+c-1})$, dont les composantes $\bar{\varphi}_t$, $t \in \mathrm{N}_{n+c}$, satisfont aux conditions :

1° $\quad \bar{\varphi}_t \neq \bar{0}$ implique $t^* = t - n \geqslant 0$ et $\geqslant j - s(t)\,\mathrm{E}$;

2° $\quad t^* = 0$ ou $t^* = j - s\,\mathrm{E}$ implique $\bar{\varphi}_t \neq \bar{0}$.

Ces conditions concernant les valeurs que prend, pour un t donné, la composante $\bar{\varphi}_t$ de $\bar{\varphi}$ parcourant $\mathrm{V}_{k,j}^{(n,c)}$ sont, visiblement, mutuellement indépendantes pour les $t \in \mathbf{N}_{n+c}$ différents. Ainsi, si U_t ($t \in \mathbf{N}_{n+c}$) est l'ensemble de ces valeurs de $\bar{\varphi}_t$ et si u_t est le nombre des éléments de U_t, $\mathrm{V}_{k,j}^{(n,c)}$ est le produit cartésien des U_t et son nombre des éléments est le produit des u_t, où t parcourt $\mathbf{N}_{n+c}$. Or, en vertu des conditions 1° et 2°, U_t est $\bar{0}$, $\bar{k} \cdot\cdot \{\bar{0}\}$ ou $\bar{k}$ (et u_t est, dans ces cas respectifs, 1, $q - 1$ ou q) selon que respectivement :

α) $\qquad t^* < \mathrm{Max}\,[0, j - s(t)\,\mathrm{E}]$;

β) $\qquad t^* = 0 \quad$ ou $\quad t^* = j - s\,\mathrm{E}$;

γ) $\qquad t^* > \mathrm{Max}\,[0, j - s(t)\,\mathrm{E}]$.

Ainsi, si ν_1, ν_2, ν_3 sont les nombres des $t \in \mathbf{N}_{n+c}$ satisfaisant aux conditions α), β) et γ) respectivement, le nombre cherché est $(q-1)^{\nu_2}\, q^{\nu_3}$. ν_2 est $= 1$ ou $= 2$ selon que $0 = j - s\,\mathrm{E}$ ou $0 \neq j - s\,\mathrm{E}$. Or $j = s\,\mathrm{E}$ implique $s(j) \geqslant m$, donc $s = m$ et $j = m\,\mathrm{E}$ (auquel cas $j - s\,\mathrm{E} = 0$). Ainsi, $(q-1)^{\nu_2} = l_j\,(q-1)$, où $l_j = q - 1$ ou 1 selon que $j <$ ou $= m\,\mathrm{E}$.

Pour calculer ν_3, partageons la réunion des intervalles

$$\mathfrak{L}_1 = (j - s\,\mathrm{E}, c - 1] \qquad \text{et} \qquad \mathfrak{L}_2 = (0, j - s\,\mathrm{E})$$

de l'axe réel, à laquelle appartiennent tous les t^* satisfaisant à la condition γ), en sous-intervalles convenables, et évaluons, pour chacun de ces sous-intervalles, le nombre de tels t^*, qui y sont. $\mathfrak{L}_1$ sera partagé en $s + 1$ sous-intervalles (dont le dernier L_0 peut être vide)

$$\mathrm{L}_0 = (j, c - 1], \qquad \mathrm{L}_1 = (j - \mathrm{E}, j],$$
$$\mathrm{L}_2 = (j - 2\,\mathrm{E}, j - \mathrm{E}], \; \ldots, \qquad \mathrm{L}_s = (j - s\,\mathrm{E}, j - (s-1)\,\mathrm{E}],$$

et $\mathfrak{L}_2$ sera partagé en $\rho - s + 1$ sous-intervalles (dont le premier peut être vide)

$$\mathrm{L}_{s+1} = [j - (s+1)\mathrm{E}, j - s\mathrm{E}), \qquad \mathrm{L}_{s+2} = [j - (s+2)\mathrm{E}, j - (s+1)\mathrm{E}), \quad \ldots,$$
$$\mathrm{L}_\rho = [j - \rho\mathrm{E}, j - (\rho - 1)\mathrm{E}), \qquad \mathrm{L}_{\rho+1} = (0, j - \rho\mathrm{E}).$$

Soit μ_i le nombre des $t^* \in \mathrm{L}_i$ $(0 \leqslant i \leqslant \rho + 1)$ satisfaisant à γ. Tout $t^* \in \mathrm{L}_0$ y satisfait, donc $\mu_0 = c - j - 1$. Si $0 < i \leqslant \rho$, on a, $i \leqslant m$ (et ceci a encore lieu pour $i = \rho + 1$ si $\rho \neq m$, autrement dit si $j \neq m\,\mathrm{E}$), donc $t^* = t - n \equiv t \pmod{p^i}$ et $s(t^*)$ est $\geqslant i$ en même temps que $s(t)$. Si $0 < i \leqslant s$, $t^* \leqslant \mathrm{L}_i$ signifie $j - i\,\mathrm{E} < t^* < j - (i-1)\,\mathrm{E}$, et un t^* satisfait à γ), autrement dit à $t^* > j - s(t)\,\mathrm{E}$ (car $t^* > 0$ est automatique), si, et seulement si $s(t) \geqslant i$, ce qui équivaut puisque $s \leqslant \rho$, à $s(t^*) \geqslant i$. Si $s < i \leqslant \rho + 1$, $t^* \in \mathrm{L}_i$ équivaut à

$$j - i\,\mathrm{E} \leqslant t^* < j - (i-1)\,\mathrm{E} \qquad \text{et} \qquad t^* > 0$$

(qui résulte déjà de la première inégalité si $i \leqslant \rho$) et, alors, $t^* > j - s(t)\,\mathrm{E}$ équivaut à $t^* \geqslant j - s(t)\,\mathrm{E}$, car $t^* = j - s(t)\,\mathrm{E}$ n'a lieu, quand $t^* > 0$, que pour $t^* = j - s\,\mathrm{E} \notin \mathrm{L}_i$. Mais, alors, un $t^* \in \mathrm{L}_i$ satisfait à γ) si, et seulement si $t^* \geqslant j - s(t)\,\mathrm{E}$, ce qui équivaut à $s(t) \geqslant i$ et, sauf si $i = \rho + 1$ et $\rho = m$, à $s(t^*) > i$. Or si $\rho = m$, on a $j = m\,\mathrm{E} = \rho\,\mathrm{E}$ et $\mathrm{L}_{\rho+1}$ est vide. Donc $s(t^*) \geqslant i$, autrement dit $t^* \equiv 0 \pmod{p^i}$, est la condition nécessaire et suffisante pour que, pour tout i tel que $0 < i \leqslant \rho + 1$, $t^* \in \mathrm{L}_i$ satisfasse à γ). Si $i \leqslant \rho$, L_i est un intervalle semi-ouvert de longueur E divisible par p^m, donc par p^i, d'où $\mu = \mathrm{E}/p^i$. Et comme

$$\mathrm{L}_{\rho+1} = (0, j - \rho\mathrm{E}) \qquad \text{et} \qquad j - \rho\,\mathrm{E} \not\equiv 0 \pmod{p^{\rho+1}} \qquad \text{si} \quad \rho < m,$$

on a
$$\mu_{\rho+1} = [j - \rho\,\mathrm{E}/p^{\rho+1}].$$

Finalement, $\nu_3 = \sum \mu_i$ est égal à

$$(c - j - 1) + (\mathrm{E}/p) + (\mathrm{E}/p^2) + \ldots + (\mathrm{E}/p^\rho) + [j - \rho\,\mathrm{E}/p^{\rho+1}].$$

11° En particulier pour calculer le nombre $\mathrm{N}_{k,j,t}^{(n)}$ des cercles de rayon $\mathfrak{P}^{n+j+t+1}$ dans $\mathrm{E}_{k,j}^{(n)}$, il suffit de poser $c = j + t - 1$, ce qui donne

$$\nu_3 = t - 2 + (\mathrm{E}/p) + \ldots + (\mathrm{E}/p^\rho) + [j - \rho\,\mathrm{E}/p^{\rho+1}],$$

donc

$$\mathrm{N}_{k,j,t}^{(n)} = \left(l_j\, q^{(\mathrm{E}/p) + (\mathrm{E}/p^2) + \ldots + (\mathrm{E}/p^\rho) + [(j - \rho\mathrm{E})/p^{\rho+1}]}\right)(q-1)\, q^{t-2},$$

et $$\mathfrak{N}^{(r)}_{k,n,j} = n\, \mathrm{N}^{(n)}_{k,j,t} / (q-1)\, q^{t-2}$$

a bien la valeur de l'énoncé du théorème 1.

12° Si $p' = p$, donc $\mathrm{E} = +\infty$, et si $f(x) \in \mathrm{E}_{k,n}$, les dérivées des termes de $f(x)$ d'exposant divisible par p sont nulles. Donc, si la différente $\mathfrak{d}_f = \mathfrak{p}^{(n+j-1):n}$ de f n'est pas nulle (ce qui équivaut à $j \neq +\infty$), le terme maximal de $f'(\alpha)$, où $f(\alpha) = 0$, provient d'un terme de $f(x)$ d'exposant premier à p, et l'on a $s = 0$. Si $m > 0$, $n\,\alpha^{n-1} = 0$, donc $j \not\equiv 0 \pmod p$ est la seule condition pour que $\mathrm{N}^{(r)}_{k,n,j} > 0$. Il y a donc lieu de poser, dans ce cas, $s\,\mathrm{E} = 0\,(+\infty) = 0$, car $m\,\mathrm{E} = 1\,(+\infty) = +\infty$, et $j < m\,\mathrm{E}$ est déjà impliqué par $j < +\infty$. Si $m = 0$, $n\,\alpha^{n-1}$ est le terme maximal de $f'(\alpha)$ et l'on a $\mathfrak{d}_f = \mathfrak{p}^{(n-1):n}$, autrement dit $j = 0$, ce qui impose pour $m\,\mathrm{E}$ la valeur 0 quand $m = 0$ et $\mathrm{E} = +\infty$.

Si $j \neq +\infty$ (ce qui assure la séparabilité des extensions considérées) les raisonnements précédents ne comportent aucune exception de validité pour $p' = p$, à condition de donner à $s\,\mathrm{E}$ et à $m\,\mathrm{E}$ la valeur 0 dans le cas ambigu $\mathrm{E} = +\infty$ et $s = 0$ respectivement $m = 0$. Si $m > 0$, l'on a

$$j < m\mathrm{E} = +\infty, \qquad \text{d'où} \quad \rho = 0 \quad \text{et} \quad l_j = q-1.$$

Donc, si $m > 0$, on a $\mathrm{N}^{(r)}_{k,n,j} = (q-1)\, q^{[j:p]}$ ou 0 selon que $j \not\equiv$ ou $\equiv 0 \pmod p$. Si $m = 0$ (extensions non-surramifiées), on a $j = 0 = m\,\mathrm{E}$, d'où $\rho = 0$ et $l_j = 1$, ce qui donne $\mathrm{N}^{(r)}_{k,n,j} = nq^{[0:p]} = n$ (résultat vrai aussi quand $p' = 0$).

Si $j = +\infty$, les conditions d'Ore $s\,\mathrm{E} \leqslant j \leqslant m\,\mathrm{E}$ exigent $m > 0$ si l'on pose $m\,\mathrm{E} = 0$ quand $m = 0$. Or, quand $p' = p$, $m > 0$ est bien la condition nécéssaire et suffisante pour qu'il existe des extensions non-séparables de degré n de k. Et alors, leur nombre (comme on voit facilement) est dénombrable, donc se représente raisonnablement par $+\infty$. D'autre part, si $j = \mathrm{E} = +\infty$, la seule interprétation raisonnable de $j : \mathrm{E}$ est de le considérer comme un nombre réel non négatif indéterminé, auquel cas $[j : \mathrm{E}]$ devient un entier indéterminé $\geqslant 0$ et, quelle que soit la valeur qu'on lui attribue, $\varepsilon(\rho)\,\mathrm{E} + [(j - \rho\,\mathrm{E}) : p^{\rho+1}]$ prend la valeur $+\infty$. D'autre part, $l_{+\infty}$, comme tout l_j, ne doit pouvoir prendre que les valeurs $q-1$ ou 1, toutes les deux > 0. Ainsi, la seule valeur raisonnable de

$$nl_j\, q^{\varepsilon(\rho)\mathrm{E} + [(j-\rho\mathrm{E}) : p^{\rho+1}]} \quad \text{quand } j = \mathrm{E} = +\infty \quad \text{est bien } +\infty.$$

13° Calculons, dans le cas $\mathfrak{p}$-adique, par sommation étendue à tous les j satisfaisant aux conditions d'Ore, $\mathfrak{N}^{(r)}_{k,n} = \sum_j \mathfrak{N}^{(r)}_{k,n,j}$. Dans ce but, divisons l'intervalle $[0, m\,\mathrm{E}]$, contenant tous les j de cette sorte, en $m+1$ sous-intervalles

$$\Lambda_0 = [0, \mathrm{E}), \qquad \Lambda_1 = [\mathrm{E}, 2\mathrm{E}), \quad \ldots, \quad \Lambda_{m-1} = [(m-1)\mathrm{E}, m\mathrm{E}),$$
$$\Lambda_m = [m\mathrm{E},\ m\mathrm{E}] = \{m\mathrm{E}\}.$$

Si j est un entier $\in \Lambda_s$, $0 \leqslant s < m$, on a

$$\rho = [j : \mathrm{E}] = s \qquad \text{et} \qquad l_j = q - 1.$$

Donc, si j satisfait aux conditions d'Ore, $\mathfrak{N}^{(r)}_{k,\,n,\,j}$ est le produit de deux facteurs $\mathfrak{N}'_s = n\,(q-1)\,(q^{\mathrm{E}})^{\varepsilon(s)}$, ne dépendant (pour k et n donnés) que de s, et $\mathfrak{N}''_j = q^{[(j - s\,\mathrm{E}) : p^{s+1}]}$, qui dépend de j. Or, j satisfait aux conditions d'Ore si, et seulement si $s\,(j)\,\mathrm{E} \leqslant j$, autrement dit $s\,(j) \leqslant s$ ce qui équivaut à $j \not\equiv 0 \pmod{p^{s+1}}$. Et, quand j parcourt les entiers $\in \Lambda_s$ non divisibles par p^{s+1}, $[(j - s\,\mathrm{E}) : p^{s+1}]$ prend toutes les valeurs $0, 1, \ldots, (\mathrm{E}/p^{s+1}) - 1$, chaque valeur étant prise $p^{s+1} - 1$ fois. Ainsi

$$\sum_{j \in \Lambda_s} \mathfrak{N}^{(r)}_{k,\,n,\,j} = \mathfrak{N}'_s \sum_{j \in \Lambda_s} \mathfrak{N}''_j$$

est le produit de

$$n\,(q-1)\,(q^{\mathrm{E}})^{\varepsilon(s)} \quad \text{par} \quad (p^{s+1}-1)\,(1 + q + \ldots + q^{(\mathrm{E}:p^{s+1})-1})$$

égal à
$$(p^{s+1}-1)\,(q^{\mathrm{E}:p^{s+1}}-1)/(q-1).$$

Comme
$$(q^{\mathrm{E}})^{\varepsilon(s)}\,q^{\mathrm{E}:p^{s+1}} = (q^{\mathrm{E}})^{\varepsilon(s+1)},$$

la somme précédente est

$$n\,(p^{s+1}-1)\,\{(q^{\mathrm{E}})^{\varepsilon(s)} - (q^{\mathrm{E}})^{\varepsilon(s+1)}\}.$$

Et
$$\sum_{j \in \Lambda_m} \mathfrak{N}^{(r)}_{k,\,n,\,j} = \mathfrak{N}^{(r)}_{k,\,n,\,m\mathrm{E}}$$

est égale à
$$n l_{m\mathrm{E}}\,(q^{\mathrm{E}})^{\varepsilon(m)} = n\,(q^{\mathrm{E}})^{\varepsilon(m)}.$$

Puisque les extensions considérées K/k sont complètement ramifiées, f_0 est aussi le degré résiduel absolu de K (autrement dit, celui de $(\mathbf{K}/\mathbf{Q}_p)$),

d'où $$f_0 \mathrm{E} = \mathrm{N} \quad \text{et} \quad q^{\mathrm{E}} = p^{f_0 \mathrm{E}} = p^{\mathrm{N}}.$$

Ainsi, l'on a

$$\mathfrak{N}_{k,n}^{(r)} = n \left\{ p^{\varepsilon(m)\mathrm{N}} + \sum_{0 \leqslant s < m} (p^{s+1} - 1)\,(p^{\varepsilon(s+1)\mathrm{N}} - p^{\varepsilon(s)\mathrm{N}}) \right\}.$$

Si l'on pose $\mathrm{P}(s) = p^{\varepsilon(s)\mathrm{N}}$, et si l'on considère l'expression entre les crochets comme une combinaison linéaire

$$\sum_s u(s)\,\mathrm{P}(s) \quad \text{des} \quad \mathrm{P}(s)\ (s = 0, 1, \ldots, m),$$

on a $$u(m) = p^m,$$
$$u(s) = (p^s - 1) - (p^{s+1} - 1) = -(p^{s+1} - p^s) \qquad \text{quand} \qquad 0 < s < m$$
et $$u(0) = -(p-1) = -(p^{0+1} - p^0).$$

Ainsi, la somme précédente $\mathrm{N}_{k,n}^{(r)}$ est

$$p^m\,\mathrm{P}(m) - \sum_{0 \leqslant s < m} (p^{s+1} - p^s)\,\mathrm{P}(s).$$

Si, maintenant, on la considère comme une combinaison linéaire $\sum_s \mathrm{U}(s)\,p^s$ des p^s $(s = 0, 1, \ldots, m)$, on voit que

$$\mathrm{U}(m) = \mathrm{P}(m) - \mathrm{P}(m-1),$$
$$\mathrm{U}(s) = \mathrm{P}(s) - \mathrm{P}(s-1) \qquad \text{si} \qquad 0 < s < m$$
et $$\mathrm{U}(0) = \mathrm{P}(0).$$

Si l'on pose $\varepsilon(-1) = -\infty$, on a

$$\mathrm{P}(-1) = p^{\varepsilon(-1)\mathrm{N}} = p^{-\infty} = 0,$$

donc on peut écrire, également,

$$\mathrm{U}(0) = \mathrm{P}(0) - \mathrm{P}(-1),$$

et la formule

$$\mathrm{U}(s) = \mathrm{P}(s) - \mathrm{P}(s-1)$$

devient universellement valable. On a donc, avec cette convention

$$\mathfrak{N}_{k,n}^{(r)} = n \sum_{0 \leq s \leq m} p^s \{ \mathrm{P}(s) - \mathrm{P}(s-1) \},$$

ce qui prouve la première formule du théorème 2.

14° **En vertu de la théorie de la ramification non-galoisienne [1], toute extension algébrique finie** K d'un corps valué complet k possède le corps d'inertie $\mathrm{K_T}$, ce corps K étant tel que $\mathrm{K_T}/k$ soit non ramifiée et que $\mathrm{K}/\mathrm{K_T}$ soit complètement ramifiée. Ainsi, toutes les extensions K/k ($\mathrm{K} \subset \mathfrak{K}$) de degré n s'obtiennent en prenant, d'abord, une extension non ramifiée arbitraire d'un degré f divisant n, et en prenant, ensuite, une extension complètement ramifiée arbitraire de degré n/f de la précédente (ces extensions étant, bien entendu, $\subset \mathfrak{K}$), et chaque extension de degré n de k est obtenue une seule fois par ce procédé. Or, si k est $\mathfrak{p}$-adique, il existe, pour tout f, une et une seule extension non-ramifiée $k^{(f)}$, donc

$$\mathfrak{N}_{k,n} = \sum_{f \mid n} \mathfrak{N}_{k^{(f)},\, n/f}^{(r)}.$$

Si $n_{0,f}$ et N_f sont les degrés par rapport à $\mathbf{Q}_p$ de $k^{(f)}$ et de son extension complètement ramifiée de degré n/f, on a

$$n_{0,f} = n_0 f \qquad \text{et} \qquad \mathrm{N}_f = (n_0 f)(n/f) = n_0\, n = \mathrm{N}.$$

Soit $f = \Delta p^{\mu}$, où $\Delta \not\equiv 0 \pmod p$. Quand f parcourt les diviseurs de n, Δ et μ (et, également, $d = h/\Delta$ et $\mu' = m - \mu$) parcourent indépendamment respectivement tous les diviseurs de h et tous les entiers du segment $[0, m]$. Et, comme $n/f = dp^{\mu'}$, on a que

$$\mathfrak{N}_{k^{(f)},\, n/f}^{(r)} = dp^{\mu'} \sum_{0 \leq s \leq \mu'} p^s \{ p^{\varepsilon(s)\mathrm{N}_f} - p^{\varepsilon(s-1)\mathrm{N}_f} \},$$

donc, en vertu de $N_f = N$, est égal à $d \sum_{0 \leqslant s \leqslant \mu} p^{s+\mu'} U(s)$. Par suite, $\mathfrak{N}_{k,n}$ est

$$\sum_{d \mid h} \sum_{0 \leqslant \mu' \leqslant m} \left(d \sum_{0 \leqslant s \leqslant \mu'} p^{s+\mu'} U(s) \right).$$

Cette expression est le produit des facteurs

$$\sum_{d \mid h} d \qquad \text{et} \qquad \sum_{0 \leqslant \mu' \leqslant m} \left(\sum_{0 \leqslant s \leqslant \mu'} p^{s+\mu'} U(s) \right),$$

et en changeant l'ordre de sommation dans le second facteur, on voit qu'il est aussi égal à

$$\sum_{0 \leqslant s \leqslant m} \left(\sum_{s \leqslant \mu' \leqslant m} (p^{\mu'}) \right) p^s U(s).$$

Comme

$$\sum_{s \leqslant \mu' \leqslant m} (p^{\mu'}) \qquad \text{est} \quad (p^{m+1} - p^s)(p-1),$$

ce second facteur est

$$\sum_{0 \leqslant s \leqslant m} \{ (p^{m+s+1} - p^{2s})/(p-1) \} \; U(s),$$

ce qui prouve la seconde formule du théorème 2.

15° Puisque h et m sont fonctions de p et n et puisque $N = n_0 n$, on voit que $\mathfrak{N}^{(r)}_{k,n}$ et $\mathfrak{N}_{k,n}$ ne dépendent que des p, n et $n_0 = (k : \mathbb{Q}_p)$. On sait que le groupe de Galois $\mathcal{G}_{\mathfrak{K}/k}$ de $\mathfrak{K}/k$ (et, également, les nombres $\mathfrak{N}^{(a)}_{k,n}$ et $\mathfrak{N}^{(g)}_{k,n}$ des extensions abéliennes, respectivement galoisiennes, de degré n de k) dépendent de certains autres paramètres, telle la présence ou l'absence dans k des racines p-ièmes primitives de l'unité. Ainsi, bien que $\mathcal{G}_{\mathfrak{K}/k}$ dépende de ces autres paramètres, le nombre de ses sous-groupes fermés d'indice fini donné n'en dépend pas (tandis que le nombre de tels sous-groupes de $\mathcal{G}_{\mathfrak{K}/k}$, qui, en plus, sont invariants ou contiennent son commutateur, peut en dépendre).

$\sum_{s \leqslant \mu} p^{s+\mu'}$ U (s). Par suite,

' U $(s)\Big)$.

$p^{s+\mu'}$ U $(s)\Big)$,

le second facteur, on voit

U (s).

$^{s}) (p - 1)$,

$)\}$ U (s),

2.

n et puisque $\mathrm{N} = n_0 n$,
les p, n et $n_0 = (k : \mathrm{Q}_p)$.
, également, les nombres
ivement galoisiennes, de
ètres, telle la présence ou
s de l'unité. Ainsi, bien
nbre de ses sous-groupes
is que le nombre de tels
nts ou contiennent son

BIBLIOGRAPHIE

[1] M. Krasner. — *Sur la primitivité des corps $\mathfrak{p}$-adiques*, Mathematica (Cluj), t. 13, 1937, p. 72-191.

[2] M. Krasner. — *Le nombre des surcorps d'un degré donné d'un corps $\mathfrak{p}$-adique*, Comptes Rendus, t. 205, 1937, p. 1026-1028.

[3] M. Krasner. — *Le nombre des surcorps primitifs et des surcorps métagaloisiens de degré donné d'un corps $\mathfrak{p}$-adique*, Comptes Rendus, t. 206, 1938, p. 876-878.

[4] M. Krasner. — *La loi de Jordan-Hölder dans les hypergroupes et les suites génératrices des corps de nombres $\mathfrak{p}$-adiques*. Duke Math. J. t. 6, 1940, p. 120-140 et t. 7, 1940, p. 121-135.

[5] M. Krasner. — *Théorie non abélienne des corps de classes pour les extensions finies et séparables des corps valués complets*, Comptes Rendus, t. 222, 1946, p. 626-628, 984-986, 1370-1372; t. 224, 1947, p. 173-175, 434-436.

[6] M. Krasner. — *Quelques méthodes nouvelles dans la théorie des corps valués complets*, Algèbre et théorie des nombres (Colloque Int. du C. N. R. S.), Paris, 1949.

[7] M. Krasner. — *Généralisation non abélienne de la théorie des corps de classes*, Proc. of the Intern. Congress of Mathematicians, Cambridge, 1950, Vol. 2, p. 71-76.

[8] M. Krasner. — *Approximation des corps valués complets de caractéristique $p \neq 0$ par ceux de caractéristique* 0, Colloque d'Algèbre Supérieure (Bruxelles, 19-22 décembre 1956), C. B. R. M.

[9] M. Krasner. — *Nombre des extensions de degré donné d'un corps $\mathfrak{p}$-adique*, Comptes Rendus, t. 254, 1962, p. 3470-3472; t. 255, 1962, p. 224-226, 1682-1684, 2342-2344, 3095-3097.

[10] Ö. Ore. — Bemerkungen zur Theorie der Differente, Math. Zeitshr. t. 25, 1926, p. 1-8.

[11] I. Safarevic. — *Sur les p-extensions*, Mat. Sbornik, Nouv. Serie, t. 20, 1947, p. 351-363.