Sur la représentation exponentielle dans les corps relativement galoisiens de nombres $\mathfrak{P}$-adiques.

Par

Marc Krasner (Paris).

Introduction.

Soit K un corps de nombres algébriques. On sait que dans un grand nombre de questions arithmétiques et même algébriques concernant K peut intervenir la structure de l'anneau de restes des entiers de K suivant les modules de la forme $\mathfrak{P}^u$, où $\mathfrak{P}$ est un idéal premier de K, en patriculier la structure de l'ensemble des éléments non nilpotents d'un tel anneau en tant que groupe abélien par rapport à la multiplication; et aussi les relations qui existent entre ces anneaux pour les u différents.

Or, ceci revient à étudier le groupe multiplicatif des unités du corps $\mathfrak{P}$-adique $K(\mathfrak{P})$ de K, et, en particulier, à en former une base exponentielle. D'ailleurs, puisque ce groupe des unités est produit direct d'un groupe de racines de l'unité de dégré premier au nombre premier (rationnel) p divisible par $\mathfrak{P}$ et du groupe des unités de $K(\mathfrak{P})$ congrues à 1 (mod $\mathfrak{P}$)[1]), on peut se borner à l'étude de ce dernier groupe.

Cette étude a été faite par M. Kurt Hensel[2]) dans une suite de

[1]) M. Hensel appelle ces unités „Einseinheiten": nous les appelerons 1-*unités* („un-unités").

[2]) Toutefois, pour le cas où K est le corps de nombres rationnels, cette étude avait été faite déjà par Euler: on la trouve exposée dans les cours élémentaires de la théorie des nombres sous le nom de la théorie des restes de puissances et des racines primitives.

travaux.[3]) La théorie de M. Hensel revient, dans ses traits éssentiels, au théorème suivant, que nous aurons à employer fréqumment au cours de ce travail:

Théorème de Hensel: *K étant un corps de nombres $\mathfrak{P}$-adiques de dégré (absolu) N, $\mathfrak{P}$ étant son idéal premier, F et E étant le dégré et l'ordre (absolus) de $\mathfrak{P}$, $\mathfrak{D}$ étant le corps des restes d'entiers de K, s'étant le plus grand nombre tel que K contienne une racine primitive p^s-ième de l'unité η, il existe N 1-unités $\varepsilon_i\,(i=1,2,\ldots,N)$ de K telles que:*

a) *toute 1-unite ε de K puisse se mettre sous la forme $\varepsilon=\eta^a\prod_{i=1}^{N}\varepsilon_i^{u_i}$, où $a, u_1, u_2,\ldots,u_N$ sont des entiers p-adiques rationnels convenables*[4]);

b) *$a, u_1, u_2\ldots,.., u_N$ étant des entiers p-adiques rationnels, $\eta^a\prod_{i=1}^{N}\varepsilon_i^{u_i}=1$ si, et seulement si à la fois $a\equiv 0 \pmod{p^s}$ et tous les $u_i\,(i\equiv 1,2,\ldots,N)$ sont* nuls. *Si K ne contient aucune racine primitive p-ième de l'unité (c'est à dire $s=0$;* on dira avec M. Hensel que *K est régulier), les ε_i peuvent être choisies de la la manière suivante:*

a) *pour tout entier q premier à p et plus petit que $E\frac{p}{p-1}$ il existe F 1-unités ε_i telles que l'ordre de ε_i-1 pour $\mathfrak{P}$ soit q; b) π étant un nombre de K d'ordre 1 en $\mathfrak{P}$, les classes (mod $\mathfrak{P}$) auxquelles appartiennent les $\frac{\varepsilon_i-1}{\pi^q}$ des F 1-unités ε_i précédemment définies forment une base de $\mathfrak{D}$* (puisqu'il y a E nombres q satisfaisant aux conditions précédentes, il y a $EF=N$ 1-unités ε_i telles que ε_i-1 ait l'ordre en $\mathfrak{P}$ égal à un de ces q, donc il n' y a aucune ε_i telle que ε_i-1 soit d'un autre ordre en $\mathfrak{P}$). *Si K contient des racines p-ièmes primitives de l'unité* (on dira, avec M. Hensel, que *K est irrégulier), on peut encore choisir les N 1-unités $\eta, \varepsilon_1, \varepsilon_2, \ldots.. \varepsilon_{N-1}$ de la manière précédente; et la $N+1^{ième}$ 1-unité $\varepsilon^*=\varepsilon_N$ peut être choisie de manière que ε^*-1 soit d'ordre $E\frac{p}{p-1}$ en $\mathfrak{P}$.*

[3]) Journ. f. d. reine u. ang. Math. 1915, t. 145, p. 92-113; 1915, t. 146 p. 189-215 cf. p. 216-228; 1917, t. 147, p. 1-15; 1923, t. 151, p. 210-212; 1937, t. 177, p. 82-93.

[4]) ε étant une 1-unité et u étant un entier p-adique rationnel, ε^u est, par définition, la somme de la série $\mathfrak{P}$-adique convergente $\sum_{i=0}^{+\infty}\binom{u}{i}(\varepsilon-1)^i$, où l'on pose $\binom{u}{i}=\frac{u(u-1)\ldots(u-i+1)}{1.2\ \ldots\ i}$ et $\binom{u}{0}=1$.

Pour ces corps, une unité $\varepsilon\equiv 1 \pmod{\mathfrak{P}^{E\frac{p}{p-1}}=(p)^{\frac{p}{p-1}}}$ est une puissance p-ième d'une 1-unité de K si, et seulement si $\frac{\varepsilon-1}{\pi^{E\frac{p}{p-1}}}\equiv\frac{p}{E}\alpha+\alpha^p \pmod{\mathfrak{P}}$, où α est un entier de K: en particulier, cette congruence n'a pas lieu pour $\varepsilon=\varepsilon^*$. Si une unité ε de K est $\equiv 1$ (mod $\mathfrak{P}^q$), elle est congrue dans les cas suivants (mod $\mathfrak{P}^{q+1}$) à la puissance p-ième d'une autre 1-unité de K: a) pour $q\leqslant E\frac{p}{p-1}$ et premier à p si et seulement si elle est congrue à 1 (mod $\mathfrak{P}^{q+1}$); *b) pour tout autre q, sauf, dans le cas des corps irréguliers, $q=E\frac{p}{p-1}$, elle l'est toujours.*

La théorie de M. Hensel avait été completée par M. Disse [5]), qui avait étudié les propriétés des logarithmes $\mathfrak{P}$-adiques des 1-unités. MM. Hensel et Hasse [6]) avaient appliqué cette théorie à l'étude du groupe multiplicatif des normes (relatives) dans un corps (relativement) kummérien de dégré p.

Quand le corps K est quelconque, la théorie de M. Hensel fournit à peu près tout ce que l'on peut dire sur la représentation exponentielle (à l'aide des exposants p-adiques rationnels) dans K. Peut-être peut-on la perfectionner par l'étude plus précise du module des logarithmes des 1-unités de K, et il existe, en effet, quelques recherches de ce genre, faites à-propos de l'étude de la forme explicite de la loi de réciprocité et liées aux idées de M. Witt. Mais si le corps est galoisien par rapport à un corps de base k, il est possible de construire une théorie de la représentation exponentielle dans K présentant une analogie plus complète avec ce qui a lieu dans le corps p-adique rationnel. Cette théorie est basée sur la généralisation suivante de la notion de l'exposant:

Soit G le groupe de Galois de K/k. Soient $\sigma_1, \sigma_2, \ldots., \sigma_m$ m éléments de G et soient $a_1, a_2, \ldots., a_m$ m entiers p-adiques rationnels. Considérons l'élément $\zeta=\sum_{i=1}^{m}a_i\sigma_i$ de l' anneau de groupe Γ engendré par G sur l'anneau $\mathfrak{E}$ des entiers p-adiques rationnels. ε étant une 1-unité, posons

[5]) Journ. f. d. reine u. ang. Math., t. 154, 1925, p. 178-193; t. 155, 1926, p. 225-250.

[6]) Math. Annalen, t. 90, 1923, p. 262-278.

$$\varepsilon^{\zeta} = \prod_{i=1}^{m} (\sigma_i \varepsilon)^{a_i} ,$$

où $\sigma_i \varepsilon$ *désigne le transformé de* ε *par l'automorphisme* σ_i *de* K/k. *On a* $\varepsilon^{\zeta_1}\varepsilon^{\zeta_2} = \varepsilon^{\zeta_1+\zeta_2}$ et $(\varepsilon^{\zeta_2})^{\zeta_1} = \varepsilon^{\zeta_1\zeta_2}$ $(\zeta_1, \zeta_2 \in \Gamma)$.

Il s'agit d'étudier le groupe multiplicatif des 1-unités de K en tant que groupe avec, comme opérateurs, les élévations aux puissances hypercomplexes $\zeta \in \Gamma$; et, en particulier, de trouver le nombre minimum des 1-unités de K telles que toute 1-unité de K puisse se mettre sous la forme d'un produit des puissances hypercomplexes de ces 1-unités.

Les premières origines de cette théorie sont antérieures aux travaux de M. Hensel. En effet, Kummer[7]) s'en était occupé déjà, sans le soupçonner, dans le cas du corps des racines p-ièmes de l'unité, à propos de ses recherches sur le premier cas du théorème de Fermat (congruences de Kummer et formule dite de Kummer-Takagi)[8]). La notion des exposants hypercomplexes avait été introduite pour ce cas par Kronecker dans sa thèse. M. Hilbert[9]) a étendu cette notion au cas général des corps relativement cycliques, et il s'en sert constamment au cours de son livre cité, et, en particulier, quand il expose la démonstration des congruences de Kummer, sans, toutefois, insister sur la quéstion même de la représentation exponentielle avec ces exposants. M. Takagi[10]) a été le premier a envisager le problème de la représentation exponentielle dans le corps des racines p-ièmes de l'unité et à le résoudre. Il ait pu montrer ainsi la véritable origine des résultats de Kummer et, en particulier, donner une démonstration simple et générale de la formule de Kummer-Takagi.

Le mérite d'avoir envisagé le problème de la représentation exponentielle à l'aide des exposants hypercomplexes dans des classes suffisamment larges de corps relativement galoisiens revient a M. Tonio Rella. Dans son travail. „Über die multiplikative Darstellung von algebraischen Zahlen eines Galois'schen Zahlkörpers für den Bereich eines

[7]) Il faut dire, toutefois, que Kummer étudiait non le groupe multiplicatif des 1-unités de ce corps, mais le groupe multiplicatif de leurs restes (mod $p^{1+\frac{2}{p-1}}$) (et, principalement (mod p)). Mais en vertu des résultats de M. Hensel, cela revient presque au même.

[8]) Journ. f. d. reine u. ang. Math., t. 44, 1852, p. 93-146; Abh. Berl. Ak., 1857, p. 1-47.

[9]) Jahresber. d. Deutsch.-Math. Ver., t. 4, 1894—1895, p. 175—546.

[10]) On the law of reciprocity in the cyclotomic corpus, Proc. of the Phys. Math. Soc. of Japan., 1922, p. 173—182.

beliebigen Primteilers" [11]) il pose et résout complètement ce problème pour le cas du corps relativement galoisien K/k complètement ramifié et de dégré (relatif) premier a p (on sait qu'un tel corps est relativement cyclique) M. Rella s'est encore occupé de ce problème pour les corps relativement cycliques de dégré (relatif) p[12]), en l'envisageant d'une manière abstraite et comme un cas particulier d'un problème plus général; pour cette raison il n'avait utilisé qu'une partie des données du problème restreint dont il s'agit, et n'était parvenu, pour ce problème, qu'à un résultat incomplet. Par contre, M. Wahlin[13]), en partant du mémoire de MM. Hensel et Hasse, cité plus haut, a résolu complètement le même problème, mais seulement pour le cas des corps relativement kummériens de dégré (relatif) p, c'est-a-dire dans l'hypothèse que k est irrégulier.

Il est à remarquer que tous les corps K/k pour lesquels la quéstion de la représentation exponentielle à l'aide des exposants hypercomplexes avait été résolue partiellement ou complètement avant le présent travail sont relativement cycliques et que les exposants hypercomplexes employés pour ces corps sont ceux introduits par M. Hilbert. Les exposants hypercomplexes généraux (dont la définition a été donnée à la page précédente) avaient été introduits par M. Nehrkorn[14]). Mais ils ne semblent pas avoir donné lieu a aucune recherche en théorie de la représentation exponentielle antérieure au présent travail.

Ce travail est consacré à l'étude de la représentation exponentielle dans les corps relativement galoisiens à l'aide des exposants $\zeta \in \Gamma$ et, en particulier, à la détermination du nombre minimum des 1-unités ε_i telles que toute 1-unité ε de K puisse se mettre sous la forme $\varepsilon = \prod_i \varepsilon_i^{\zeta_i}$ $(\zeta_i \in \Gamma)$. Les résultats de ce travail peuvent être appliqués à la recherche de la forme explicite de la loi de réciprocité, ainsi qu'à certaines autres quéstions, mais, à quelques exceptions près, ces applications seront exposées ailleurs.

La partie du travail publiée dans le présent fascicule des Acta Arithmetica est consacrée au cas où le corps K/k est sans ramifications su-

[11]) Journ. f. d. reine u. ang. Math, t. 150, 1920, p. 157-174.

[12]) „Die Abel'sche Operatorgruppen" Journ. f. d. reine u. ang. Math., t, 167, 1932, p. 235-247.

[13]) Journ. f. d. reine u. ang. Math., t. 167, 1932, p. 122.

[14]) Abh. Hamb. Seminar, t. 9., 1933, p. 318.

périeures et aux quéstions du cas général ayant une nature similaire. La seconde partie, consacrée au passage de ce cas particulier au cas général, sera publiée plus tard.

Notations

Nous allons désigner par k un corps de nombres $\mathfrak{p}$-adiques et par K un surcorps relativement galoisien de k. Les idéaux premiers de k, K seront désignés respectivement par $\mathfrak{p}$, $\mathfrak{P}$. On notera $\Omega(k)$ et $\Omega(K)$ les corps des restes d'entiers de k, K suivant leurs idéaux premiers; p étant le nombre premier rationnel divisible par $\mathfrak{p}$, on désignera par Ω_a le champ de Galois (de caracteristique p) de p^a éléments.

Le dégré et l'ordre de $\mathfrak{P}$ dans K/k seront notés f, e; le dégré et l'ordre absolus de $\mathfrak{p}$ dans k seront notés f_0, e_0 et ceux de $\mathfrak{P}$ dans K seront notés $F = f_0 f$ et $E = e_0 e$. Le dégré de K/k, le dégré absolu de k et celui de K seront notés respectivement n, n_0, N. On désignera par Z, T, V les groupes de décomposition, d'inertie et de ramification de K/k. On notera $\overline{Z}$, $\overline{T}$ les groupes Z/V et T/V.

Le p. g. c. d. de deux entiers rationnels a, b sera noté $[a, b]$ et leur p. p. c. m. sera noté (a, b). On posera $e = h p^{\mu}$, où $[h, p] = 1$. $a|b$ signifie „a divise b“. Nous désignons par $\mathfrak{E}$ l'anneau des entiers p-adiques rationnels et par $\mathfrak{E}_k$ l'anneau des entiers de k; l'anneau de groupe engendré par Z sur $\mathfrak{E}$ sera noté Γ, et celui engendré sur $\mathfrak{E}_k$ par Γ_k. Les anneaux engendrés par $\overline{Z}$ sur Ω_1 et sur $\Omega(k)$ seront notés respectivement par $\overline{\Gamma}$ et $\overline{\Gamma}_k$. Si ζ est un élément de Γ ou de Γ_k, l'element correspondant de $\overline{\Gamma}$ respectivement $\overline{\Gamma}_k$ sera designe par $\overline{\zeta}$.

Les signes $\cap, \cup, \supset, \subset, \in$ auront le sens habituel de la théorie des ensembles. Les signes $+, -$ et $\cdot$ ne seront employés que pour des opérations algébriques. La somme directe des modules $A, B, C, \ldots$, admettant, eventuelement, certains opérateurs, sera désignée par $A \oplus B \oplus C \oplus \ldots$

La norme absolue de $\mathfrak{p}$ sera notée $\mathfrak{o}$, celle $\mathfrak{P}$ sera notée $\widetilde{\Omega}$.

L'ordre en $\mathfrak{P}$ d'un nombre α de K sera désigné par $\omega(\alpha)$; Q étant un anneau, $Q[x]$ désignera l'anneau des polynomes en x à coefficients dans Q; $\{a_1, a_2, \ldots, a_m\}$ notera l'ensemble des éléments $a_1, a_2, \ldots, a_m$, $Q/\overline{Q}$ étant un corps, l'ensemble de tous les isomorphismes de $Q/\overline{Q}$ avec ses conjugués sera noté $G_{Q/\overline{Q}}$. Un intervalle ouvert de a à b sera noté (a, b). Le même intervalle fermé sera noté $[a, b]$. Enfin, le même intervalle ouvert en a et fermé en b sera noté $(a, b]$.

λ étant une fonction, transformation, correspondance, opération etc. s'appliquant à certains objets a, et A étant un ensemble d'objets auxquels λ s'applique, λA désignera l'ensemble de tous les λa distincts tels que $a \in A$. Λ etant un ensemble d'opérations λ s'appliquant à tous les objets a appartennant à un ensemble A, ΛA désignera l'ensemble de tous les λa distincts tels que $\lambda \in \Lambda$ et $a \in A$.

§ 1 - Un théorème sur les groupes abéliens d'ordre fini avec un anneau d'opérateurs.

Soit $\mathfrak{A}$ un groupe abélien d'ordre fini avec un anneau d'opérateurs Γ (Γ — groupe). Nous emploierons la notation additive, c'est-à-dire que l'opération de composition dans $\mathfrak{A}$ sera notée $+$. L'opéré d'un $a \in \mathfrak{A}$ par un $\gamma \in \Gamma$ sera noté γa. Si, dans la suite du travail, on aura à employer pour des semblables groupes la notation multiplicative, l'opéré de $a \in \mathfrak{A}$ par un $\gamma \in \Gamma$ sera noté a^{γ}.

Un sous ensemble $\overline{A}$ de $\mathfrak{A}$ s'appelera une Γ - *base de* $\mathfrak{A}$ si $\sum_{a \in \overline{A}} \Gamma a = \mathfrak{A}$.

Une Γ - base de $\mathfrak{A}$ dont le nombre d'éléments est le plus petit possible sera dite *de rang minimum* et ce nombre d'éléments s'appellera le Γ - *rang de* $\mathfrak{A}$.

Soit

$$\mathfrak{A} = A_0 \supset A_1 \supset \ldots \quad \ldots \supset A_q = \{0\} \tag{1}$$

une chaîne (au sens large) de sous - Γ - groupes de $\mathfrak{A}$ (c'est - à - dire que tout A_i, $0 \leqslant i \leqslant q$, est un sous-groupe de $\mathfrak{A}$ et $\Gamma A_i = A_i$). La somme directe $\mathfrak{N}$ de tous les $\mathfrak{N}_i = A_i / A_{i+1}$ $(i = 0, 1, \ldots, q-1)$ est encore un Γ - groupe abélien d'ordre fini, qui s'appellera *image de* $\mathfrak{A}$ *par la chaîne* (1).

Théorème 1: *Le* Γ - *rang d'un* Γ - *groupe abélien d'ordre fini ne dépasse pas le* Γ - *rang d'une quelconque de ces images.*

Démonstration: a) Prouvons le théorème dans le cas où le Γ - rang de l'image $\mathfrak{N}$ de $\mathfrak{A}$ est 1, c'est-à-dire quand il existe un $\alpha = \bigoplus_{0 \leqslant i < q} \alpha_i$ ($\alpha_i \in \mathfrak{N}_i$ [15]) tel que $\Gamma \alpha = \mathfrak{N}$. Supposons qu'on ait prouvé pour un i, $0 \leqslant i < q$,

[15]) $\bigoplus_{0 \leqslant i < q} \alpha_i$ désigne l'élément de $\mathfrak{N}$ dont la composante dans $\mathfrak{N}_i$ est α_i.

l'existence d'un $a_i \in A$ et d'un $\gamma_i \in \Gamma$ tels que

$1^0)$ $\Gamma\, a_i + A_i = A$

$2^0)$ $\gamma_i\, a_i \in A_i$ et $\gamma_i \alpha_j = 0$ ou $= \alpha_j$ suivant que $j < i$ ou $j \geqslant i$.

Prouvons l'existence d'un $a_{i+1} \in A$ et d'un $\gamma_{i+1} \in \Gamma$ satisfaisant aux mêmes conditions pour $i+1$. Posons

$$C_m = \gamma_i^m \mathfrak{A}_i .$$

Puisque $\gamma_i \mathfrak{A}_i \subseteq \mathfrak{A}_i$, on a $C_{m+1} = \gamma_i^{m+1} \mathfrak{A}_i = \gamma_i^m (\gamma_i \mathfrak{A}_i) \subseteq \gamma_i^m \mathfrak{A}_i = C_m$, donc $\mathfrak{A}_i = C_0 \supseteq C_1 \supseteq C_2 \supseteq \ldots$ $\mathfrak{A}_i$ étant d'ordre fini, il existe un m tel que $C_m = C_{m+1} = \gamma_i C_m$. Donc γ_i produit une application de l'ensemble fini C_m sur lui-même, donc une permutation P de C_m; d'autre part, γ_i^m transforme tout élément de $\mathfrak{A}_i$ en un élément de C_m. Donc si M est un multiple de l'ordre de P tel que $M \geqslant m$, $\gamma^* = \gamma_i^M$ transforme tout élément de $\mathfrak{A}_i$ en un élément de C_m, et conserve les éléments de C_m. Soit a' un élément de α_i (regardé comme une classe (mod A_{i+1}) dans A_i). Posons

$$a_{i+1} = (1 - \gamma^{*2})\, a_i + a' .$$

On a, puisque $\gamma^{*2} a_i \in A_i$ et $a' \in A_i$, que $a_{i+1} \equiv a_i \pmod{A_i}$, donc

$$\Gamma\, a_{i+1} + A_i = \Gamma\, a_i + A_i = A .$$

D'autre part

$$\gamma^{*2} a_{i+1} = \gamma^{*2} a_i - \gamma^{*4} a_i + \gamma^{*2} a' .$$

Or $\gamma^* a_i \in A_i$, donc la classe de $\gamma^* a_i \pmod{A_{i+1}}$ fait partie de $\mathfrak{A}_i$. Donc la classe de $\gamma^{*2} a_i = \gamma^* (\gamma^* a_i) \pmod{A_{i+1}}$ fait partie de C_m, donc γ^*, et, à fortiori, γ^{*2} conserve cette classe. Donc $\gamma^{*4} a_i \equiv \gamma^{*2} a_i \pmod{A_{i+1}}$. D'autre part puisque $a' \in \alpha_i$, et puisque γ_i, et à fortiori $\gamma^{*2} = \gamma_i^{2M}$, conserve α_i, on a $\gamma^{*2} a' \equiv a' \pmod{A_{i+1}}$; donc

$$\gamma^{*2} a_{i+1} \equiv a' \pmod{A_{i+1}}$$

et $\gamma^{*2} a_{i+1} + A_{i+1} = a' + A_{i+1} = \alpha_i$. Puisque $\Gamma \alpha_i = \mathfrak{A}_i$, on a $\Gamma \gamma^{*2} a_{i+1} + A_{i+1} = A_i$, donc

$$A = \Gamma\, a_{i+1} + A_i = \Gamma\, a_{i+1} + \Gamma\, \gamma^{*2} a_{i+1} + A_{i+1} = (\Gamma + \Gamma \gamma^{*2})\, a_{i+1} + A_{i+1} = \Gamma\, a_{i+1} + A_{i+1},$$

parce que, Γ étant un groupe additif, $\Gamma + \Gamma \gamma^{*2} = \Gamma$.

Considérons un élément $\beta = \bigoplus \beta_j$ de $\mathfrak{A}$ tel que $\beta_i = 0$ et $\beta_j = \alpha_j$ si $0 \leqslant j < q$

$j \geqslant i+1$. Puisque $\Gamma \alpha = \mathfrak{A}$, il existe un $\gamma' \in \Gamma$ tel que $\gamma' \alpha = \beta$, donc $\gamma' \alpha_j = \beta_j$ $(j = 0,1, \ldots, q-1)$. Posons

$$\gamma_{i+1} = \gamma' \gamma^{*2} .$$

On a $\gamma_{i+1} (a_{i+1} + A_{i+1}) = \gamma' (\gamma^{*2} a_{i+1} + A_{i+1}) = \gamma' \alpha_i = \beta_i = 0$, donc

$$\gamma_{i+1}\, a_{i+1} \in A_{i+1},$$

et $\gamma_{i+1} \alpha_j = \gamma' (\gamma^{*2} \alpha_j)$; donc si $j < i$, on a $\gamma_{i+1} \alpha_j = \gamma' 0 = 0$; $\gamma_{i+1} \alpha_i = \gamma' \alpha_i = \beta_i = 0$; si $j \geqslant i+1$, $\gamma_{i+1} \alpha_j = \gamma' \alpha_j = \beta_j = \alpha_j$. Donc a_{i+1} et γ_{i+1} satisfont bien aux conditions $1^0)$ et $2^0)$ pour $i+1$.

Comme $a_0 = 0$ et $\gamma_0 = 1$ satisfont bien aux conditions $1^0)$ (parce que $\Gamma . 0 + A_0 = A_0 = A$) et $2^0)$ (parce que $1 . 0 = 0 \in A_0$ et $1 . \alpha_j = \alpha_j$ pour tout $j = 0,1, \ldots . q-1$) pour $i = 0$, on voit qu'il existe un $a_q \in A$ et un $\gamma_q \in \Gamma$ satisfaisant aux mêmes conditions pour $i = q$. Or la conditions $1^0)$ s'écrit, puisque $A_q = \{0\}$,

$$\Gamma a_q = A$$

et le Γ-rang de A est 1.

b) Considérons le produit direct A^r de r Γ-groupes égaux à A. Ce produit direct qui peut être regardé comme l'ensemble de tous les systèmes de valeurs possibles $x_1 = a_1$, $x_2 = a_2$, $\ldots$, $x_r = a_r$ de r variables $x_1, x_2, \ldots, x_r$ parcourant indépendamment A, est aussi un groupe abélien d'ordre fini si l'on pose $(a_1, a_2, \ldots, a_r) + (b_1, b_2, \ldots \ldots, b_r) = (a_1 + b_1, a_2 + b_2, \ldots, a_r + b_r)$ $(a_1, a_2, \ldots, a_r, b_1, b_r, \ldots \ldots, b_r \in A)$. Soit Γ_r l'anneau das matrices carrées d'ordre r dans Γ; désignons par $\gamma = (\gamma_j^{(i)})$ $\left(\gamma_j^{(i)} \in \Gamma;\ \begin{matrix} i = 1, 2, \ldots, r. \\ j = 1, 2, \ldots, r, \end{matrix}\right)$ la transformation linéaire de A^r de matrice γ, c'est-à-dire l'opérateur

$$(a_i) \to \left(\sum_{j=1}^{r} \gamma_j^{(i)} a_j \right) \quad (i = 1,2, \ldots \ldots, r)$$

de A^r. De cette manière A^r admet Γ_r comme anneau d'opérateurs. Si

$\overline{A}$ est un sous-Γ-groupe de A, manifestement $\overline{A}^r$ est un sous-Γ-groupe de A^r. A^r est de Γ_r-rang 1 si, et seulement si le Γ rang de A est $\leqslant r$, $\mathfrak{A}$ étant une image de A par la chaine (1), $\mathfrak{A}^r$ est aussi, pour la même raison et de la même manière que A, un Γ_r-groupe. $\mathfrak{A}^r$ est l'image de A^r par la chaine des sous—Γ_r-groupes de A^r

$$A^r = A_0{}^r \supset A_1{}^r \supset \ldots\ldots \supset A_q{}^r = \{0\},$$

car
$$\mathfrak{A}_i{}^r = (A_i/A_{i+1})^r = A_i{}^r/A_{i+1}^r.$$

Supposons que le Γ-rang de $\mathfrak{A}$ soit r. Alors le Γ_r-rang de $\mathfrak{A}^r$ est 1. $\mathfrak{A}^r$ étant une image de Γ_r-groupe abélien d'ordre fini A^r, A^r est aussi, en vertu de a), de Γ_r-rang 1; donc le Γ-rang de A ne dépasse par r, c'est-à-dire ne dépasse pas le rang de $\mathfrak{A}$, et tout est prouvé.

§ 2 — Exposants hypercomplexes. Un théorème sur la représentation exponentielle. Facteurs hypercomplexes.

Un théorème sur la représentation factorielle.

Soient k un corps de nombres $\mathfrak{p}$-adiques et K une extension galoisienne de dégré fini de k. Soient $\mathfrak{P}, \mathfrak{p}$ et p respectivement l'idéal premier de K, celui de k et le nombre premier rationnel qu'ils divisent. Soit G le groupe de Galois de K/k; a étant un entier p-adique rationnel et ε étant une 1-unité de K, on sait que ε^a est aussi une 1-unité bien définie de K à savoir la somme de la série $\mathfrak{P}$-adique convergente.

$$\sum_{i=0}^{+\infty} \left\{ \begin{matrix} a \\ i \end{matrix} \right\} (\varepsilon - 1)^i$$

où $\left\{ \begin{matrix} a \\ 0 \end{matrix} \right\} = 1$ et, si $i > 0$, $\left\{ \begin{matrix} a \\ i \end{matrix} \right\} = \dfrac{a\ (a-1)\ \ldots\ldots\ (a-i+1)}{1.\ 2\ \ldots\ldots\ i}$.

Soit Γ l'anneau de groupe engendré par G sur l'anneau $\mathfrak{E}$ des entiers p-adiques rationnels. $\zeta = \sum_i a_i \sigma_i$ étant un élément de Γ, et ε étant une 1-unité de K (donc, ses conjugués par rapport à k le sont aussi) posons

$$\varepsilon^{\zeta} = \prod_i (\sigma_i\, \varepsilon)^{a_i}.$$

ε^{ζ} s'appellera *puissance hypercomplexe* de ε *d'exposant (hypercomplexe)* ζ. On a, manifestement,

$$\varepsilon^{\zeta_1}\, \varepsilon^{\zeta_2} = \varepsilon^{\zeta_1 + \zeta_2};\quad (\varepsilon_1\, \varepsilon_2)^{\zeta} = \varepsilon_1{}^{\zeta}\, \varepsilon_2{}^{\zeta};\quad \left(\varepsilon^{\zeta_2}\right)^{\zeta_1} = \varepsilon^{\zeta_1\, \zeta_2}.$$

Un groupe multiplicatif $\mathfrak{U}$ de 1-unités de K s'appellera Γ-groupe de K si $\mathfrak{U}^{\Gamma} = \mathfrak{U}$, c'est-à-dire si $\mathfrak{U}^{\mathfrak{S}} = \mathfrak{U}$ et si $\mathfrak{U}$ est conservé par tout automorphisme de K/k. Soit R_q le rayon de $\mathfrak{P}^q$ dans K, c'est-à-dire le groupe des 1-unités de K congrues à 1 (mod $\mathfrak{P}^q$). Manifestement $R_q{}^{\mathfrak{S}} = R_q$; Si $\sigma \in G$, on a $\sigma\, \mathfrak{P} = \mathfrak{P}$, donc, si $\varepsilon \equiv 1 \pmod{\mathfrak{P}^q}$, on a aussi

$$\sigma\, \varepsilon \equiv 1 \pmod{\sigma\, \mathfrak{P}^q = \mathfrak{P}^q};$$

donc R_q est un Γ-groupe de K. $\mathfrak{U}$ étant un Γ-groupe de K, on posera $\mathfrak{U}_q = \mathfrak{U} \cap R_q$. C'est, manifestement, encore un Γ-groupe.

$\mathfrak{U}$ est à remarquer que tout groupe multiplicatif $\mathfrak{U}$ de 1-unités de K tel que $\mathfrak{U}^{\mathfrak{S}} = \mathfrak{U}$ est fermé au sens de la topologie $\mathfrak{P}$-adique. En effet, en vertu du théorème de Hensel, il existe un nombre fini de 1-unités $\varepsilon_1, \varepsilon_2, \ldots\ldots, \varepsilon_\nu$ de K telles que

$$\varepsilon_1{}^{\mathfrak{S}}\, \varepsilon_2{}^{\mathfrak{S}} \ldots\ldots \varepsilon_\nu{}^{\mathfrak{S}} = R_1.$$

R_1 est donc un groupe abélien avec un module d'opérateurs $\mathfrak{S}$ et de rang fini par rapport à ce module. $\mathfrak{U}$ étant un sous-groupe de R_1, admettant ce module d'opérateurs, il est aussi de rang fini par rapport à $\mathfrak{S}$. Donc il existe ν' éléments $\varepsilon'_1, \varepsilon'_2, \ldots\ldots, \varepsilon'_{\nu'}$ de $\mathfrak{U}$ tels que

$$\mathfrak{U} = \varepsilon_1{}'^{\mathfrak{S}}\, \varepsilon'_2{}^{\mathfrak{S}} \ldots\ldots\ \varepsilon'_{\nu'}{}^{\mathfrak{S}}.$$

Soit $\overline{\varepsilon}_1, \overline{\varepsilon}_2, \ldots\ldots, \overline{\varepsilon}_n$ une suite convergente (au sens $\mathfrak{P}$-adique) d'éléments de $\mathfrak{U}$; soit

$$\overline{\varepsilon}_n = \varepsilon_1{}'^{a_2^{(n)}}\, \varepsilon_2{}'^{a_2^{(n)}} \ldots\ldots\ \varepsilon'_{\nu'}{}^{a'^{(n)}_{\nu'}} \qquad (a_j^{(n)} \in \mathfrak{E}).$$

$\mathfrak{E}$ étant borné (au sens $\mathfrak{P}$-adique), on peut extraire une suite partielle $\overline{\varepsilon}_{n_i}$ de la suite $\overline{\varepsilon}_n$ telle que les ν' suites $a_j^{(n_i)}$ $(j = 1, 2, \ldots\ldots, \nu')$ d'entiers

p-adiques rationnels convergent simultanément. Soit $a_j = \lim_{i \to +\infty} a_j^{(n_i)}$, alors

$\bar{\varepsilon} = \varepsilon_1'^{a_1} \varepsilon_2'^{a_2} \ldots\ldots \varepsilon_{\nu'}'^{a_{\nu'}}$ est encore un élément de $\mathfrak{U}$ et

$$\bar{\varepsilon} = \lim_{i \to +\infty} \bar{\varepsilon}_{n_i} = \lim_{n_i \to +\infty} \bar{\varepsilon}_{n_i} = \lim_{n \to +\infty} \bar{\varepsilon}_n.$$

En particulier, les Γ-groupes de K sont fermés.

Soit ε une 1-unité de K. On a

$$\varepsilon^p = 1 + \sum_{i=1}^{p-1} \left\{ \begin{matrix} p \\ i \end{matrix} \right\} (\varepsilon - 1)^i + (\varepsilon - 1)^p;$$

donc, si $\varepsilon \in R_q$, $\varepsilon^p \equiv 1 \pmod{\mathfrak{P}^q, [p, \mathfrak{P}^q]}$ donc, à fortiori $\pmod{\mathfrak{P}^{q+1}}$, et $\varepsilon^p \in R_{q+1}$.

Si π est un nombre de K divisible par $\mathfrak{P}$ et non par $\mathfrak{P}^2$, et si σ est un élément du groupe de ramification V de K/k, on a

$$\frac{\sigma\pi}{\pi} \equiv 1 \pmod{\mathfrak{P}}.$$

Donc $\frac{\sigma\pi^q}{\pi^q} = \left(\frac{\sigma\pi}{\pi}\right)^q \equiv 1 \pmod{\mathfrak{P}}$. Si $\varepsilon \in R_q$, $\frac{\varepsilon - 1}{\pi^q}$ est entier, donc $\sigma\left(\frac{\varepsilon-1}{\pi^q}\right) \equiv \frac{\varepsilon-1}{\pi^q} \pmod{\mathfrak{P}}$.

Donc $\frac{\sigma\varepsilon - 1}{\varepsilon - 1} \equiv \frac{\sigma\pi^q}{\pi^q} \equiv 1 \pmod{\mathfrak{P}}$. Et puisque $\varepsilon - 1 \equiv 0 \pmod{\mathfrak{P}^q}$, on a $\sigma\varepsilon - 1 \equiv \varepsilon - 1 \pmod{\mathfrak{P}^{q+1}}$ et $\sigma\varepsilon \equiv \varepsilon \pmod{\mathfrak{P}^{q+1}}$.

Donc

$$\varepsilon^{\sigma-1} \equiv \frac{\sigma\varepsilon}{\varepsilon} \equiv 1 \pmod{\mathfrak{P}^{q+1}}$$

et $\varepsilon^{\sigma-1} \in R_{q+1}$.

Envisageons l'idéal (forcement bilatère, parce que ν appartient au centre de Γ et V est invariant dans G) $\mathfrak{v} = \Gamma p + \Gamma(V-1)$ de Γ. Si $\varepsilon \in R_q$ et si $\zeta \in \mathfrak{v}$, manifestement $\varepsilon^\zeta \in R_{q+1}$. Donc, si $\mathfrak{U}$ est un Γ-groupe contenu dans R_q, $\mathfrak{U}^* = \mathfrak{U}^{\mathfrak{v}}$ est contenu dans R_{q+1}. Si l'on pose $\mathfrak{U}^{(0)} = \mathfrak{U}$ et si l'on définit $\mathfrak{U}^{(i)}$ par la formule de récurrence $\mathfrak{U}^{(i)} = (\mathfrak{U}^{(i-1)})^{\mathfrak{v}}$, on voit que, sûrement,

$$\mathfrak{U}^{(i)} \subseteq R_i.$$

Soient $\mathfrak{U}$ un Γ-groupe de K et $\overline{\mathfrak{U}}$ un sous-Γ-groupe de $\mathfrak{U}$. Un ensemble $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r\}$ d'éléments de $\mathfrak{U}$ s'appellera Γ-*base de* $\mathfrak{U}/\overline{\mathfrak{U}}$ si $\mathfrak{U} = \varepsilon_1^\Gamma \varepsilon_2^\Gamma \ldots\ldots \varepsilon_r^\Gamma \overline{\mathfrak{U}}$. La plus petite valeur que peut prendre le rang d'une Γ-base de $\mathfrak{U}/\overline{\mathfrak{U}}$ s'appellera Γ-*rang* de $\mathfrak{U}/\overline{\mathfrak{U}}$ et les Γ-bases de $\mathfrak{U}/\overline{\mathfrak{U}}$ ayant ce rang seront dites *de rang minimum.*

Lemme 1: Le Γ-rang de $\mathfrak{U}/\overline{\mathfrak{U}}$ *est égal à celui de* $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$.

Démonstration: Considérons une base de rang minimum de $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$. Soit $\mathfrak{U}'$ le sous-Γ-groupe de $\mathfrak{U}$ engendré par cette base et par $\overline{\mathfrak{U}}$. On a $\mathfrak{U}'\mathfrak{U}^* = \mathfrak{U}$. ε étant un élément de $\mathfrak{U}$, il existe, par suite, des éléments ε' de $\mathfrak{U}'$ tels que $\frac{\varepsilon}{\varepsilon'}$ soit dans $\mathfrak{U}^*$. Deux cas peuvent se présenter: ou bien, pour tout q il existe des ε' de la forme précédente tels que $\frac{\varepsilon}{\varepsilon'} \in \mathfrak{U}^{(q)}$. Mais alors la limite ($\mathfrak{P}$-adique) de $\frac{\varepsilon}{\varepsilon'}$ pour ces ε' sera 1 et la limite des ε' est ε. Dans ces conditions, puisque le Γ-groupe $\mathfrak{U}'$ est fermé, $\varepsilon \in \mathfrak{U}'$; Ou bien il existe un q tel que, pour aucun $\varepsilon' \in \mathfrak{U}'$, $\frac{\varepsilon}{\varepsilon'}$ ne soit pas dans $\mathfrak{U}^{(q)}$, mais que, pour un ε' convenable $\frac{\varepsilon}{\varepsilon'} \in \mathfrak{U}^{(q-1)}$. Mais $\mathfrak{U}^{(q-1)} = \mathfrak{U}^{\mathfrak{v}^{q-1}} = (\mathfrak{U}'\mathfrak{U}^*)^{\mathfrak{v}^{q-1}} = (\mathfrak{U}'\mathfrak{U}^{\mathfrak{v}})^{\mathfrak{v}^{q-1}} = \mathfrak{U}'^{\mathfrak{v}^{q-1}}\mathfrak{U}^{\mathfrak{v}^q} \subseteq \mathfrak{U}'\mathfrak{U}^{(q)}$. Il existe donc un $\varepsilon'' \in \mathfrak{U}'$ et un $\varepsilon^* \in \mathfrak{U}^{(q)}$ tels que $\frac{\varepsilon}{\varepsilon'} = \varepsilon''\varepsilon^*$. Donc $\frac{\varepsilon}{\varepsilon'\varepsilon''} \in \mathfrak{U}^{(q)}$ et $\varepsilon'\varepsilon'' \in \mathfrak{U}'\mathfrak{U}' = \mathfrak{U}'$ et ce cas est impossible. Donc tout $\varepsilon \in \mathfrak{U}$ est élément de $\mathfrak{U}'$ et la Γ-base considérée de $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$ est aussi Γ-base de $\mathfrak{U}/\overline{\mathfrak{U}}$. Comme, inversement, toute Γ-base de $\mathfrak{U}/\overline{\mathfrak{U}}$ en est une de $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$, on voit que les Γ-rangs de $\mathfrak{U}/\overline{\mathfrak{U}}$ et de $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$ sont égaux.

C. Q. F. D.

Or $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$ est un Γ-groupe abélien qui est, en vertu du théorème de Hensel, d'ordre fini; quelque soit q, $\mathfrak{U}_q\overline{\mathfrak{U}}\,\mathfrak{U}^*/\overline{\mathfrak{U}}\,\mathfrak{U}^*$ est un sous-Γ-groupe de $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$. Donc, si l'ensemble $q_1, q_2, \ldots\ldots, q_s$ des entiers naturels com-

prend tous les q tels que. $\mathfrak{U}_q \overline{\mathfrak{U}} \mathfrak{U}^* \neq \mathfrak{U}_{q+1} \mathfrak{U} \overline{\mathfrak{U}}^*$ (de tels ensembles finis de q_i existent parce que $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$ est d'ordre fini et parce qu'il existe des q tels que $\mathfrak{U}^* \supseteq \mathfrak{U}_q$) le produit direct U[16]) des groupes

$$\mathfrak{U}_{q_i} = \mathfrak{U}_{q_i} \overline{\mathfrak{U}}\, \mathfrak{U}^* / \mathfrak{U}_{q_{i+1}} \overline{\mathfrak{U}}\, \mathfrak{U}^* = \mathfrak{U}_{q_i} \overline{\mathfrak{U}}\, \mathfrak{U}^* / \mathfrak{U}_{q_{i+1}} \overline{\mathfrak{U}}\, \mathfrak{U}^*$$

est une image de $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$. Donc, en appliquant le théorème 1, on trouve le

Théorème 2: Le Γ-rang de $\mathfrak{U}/\overline{\mathfrak{U}}$ ne dépasse pas celui de U.

Démonstration: En vertu du lemme 1 le Γ-rang de $\mathfrak{U}/\overline{\mathfrak{U}}$ est égal à celui de $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$. Et ce dernier ne dépasse pas, en vertu du théorème 1, le Γ-rang de l'image U de $\mathfrak{U}/\overline{\mathfrak{U}}\,\mathfrak{U}^*$.

Soit $\overline{K}$ un sous-corps[17]) de K, et soit $\overline{\mathfrak{P}}$ l'idéal premier de $\overline{K}$. Considérons l'anneau de groupe $\Gamma_{\overline{K}}$ engendré par G sur l'anneau $\mathfrak{E}_{\overline{K}}$ des entiers de $\overline{K}$. $\zeta = \sum_i a_i \sigma_i$ ($a_i \in \mathfrak{E}_{\overline{K}}$, $\sigma_i \in G$) étant un élément de $\Gamma_{\overline{K}}$ et α étant un nombre de K, posons

$$\zeta\,\alpha = \sum_i a_i \,.\, \sigma_i \alpha$$

ζ sera dit *facteur hypercomplexe.* Un module M dans K tel que $\Gamma_{\overline{K}}\, M = M$ et borné au sens de la topologie $\mathfrak{P}$-adique sera dit $\Gamma_{\overline{K}}$-*module de* K. M étant un $\Gamma_{\overline{K}}$-module de K et $\overline{M}$ étant un de ces sous-$\Gamma_{\overline{K}}$-modules, $M/\overline{M}$ est un module admettant $\Gamma_{\overline{K}}$ comme anneau d'opérateurs. Un ensemble $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ d'éléments de M s'appellera $\Gamma_{\overline{K}}$-*base de* $M/\overline{M}$ si $\sum_{i=1}^{r} \Gamma_{\overline{K}}\, \alpha_i + \overline{M} = M$. Soit $\mathfrak{v} = \overline{\mathfrak{P}}\, \Gamma_{\overline{K}} + \Gamma_{\overline{K}}(V-1)$ et soit $M^* = \mathfrak{v} M$. Alors on prouve, comme précédemment, que le $\Gamma_{\overline{K}}$-rang de $M/\overline{M}$ est égal à celui de $M/(\overline{M}+M^*)$. Ce dernier module est un $\Gamma_{\overline{K}}$-groupe abélien d'ordre fini. Donc, puisque M est borné au sens $\mathfrak{P}$-adique, il existe un entier q' (positif, négatif ou nul) tel que $\mathfrak{P}^{q'} \supseteq M$ et un entier q'' tel qne $\overline{M} + M^* \supseteq M^* \supseteq M \cap \mathfrak{P}^{q''}$. Pour tout q, $\Gamma_{\overline{K}} \mathfrak{P}^q = (\Gamma_{\overline{K}} \mathfrak{P})^q = \mathfrak{P}^q$, donc, si l'on

[16]) qui ne dépend pas, à Γ-isomorphie prés, du choix de l'ensemble des q_i satisfaisant à cette condition.

[17]) on n'au.a à regarder dans la suite du travail que le cas $\overline{K} = k$.

pose $M_q = M \cap \mathfrak{P}^q$, on a $\Gamma_{\overline{K}}\, M_q = M_q$ et $M_q + \overline{M} + M^*/(\overline{M} + M^*)$ est un sous-$\Gamma_{\overline{K}}$-module de $M/(\overline{M}+M^*)$. D'autre part, il existe des ensembles finis $q_1, q_2, \ldots, q_s$ d'entiers (par exemple l'ensemble de tous les entiers $q, q' \leqslant q \leqslant q''$) qui comprennent tous les q tels que $M_q + \overline{M} + M^* \neq M_{q+1} + \overline{M} + M^*$ (et, en particulier, $M_{q_1} + \overline{M} + M^* = M$, $M_{q_s} \subseteq \overline{M} + M^*$). Donc, la somme directe μ des $\mu_{q_i} = (M_{q_i} + \overline{M} + M^*)/(M_{q_{i+1}} + \overline{M} + M^*) = (M_{q_i} + \overline{M} + M^*)/(M_{q_{i+1}} + \overline{M} + M^*)$ ($i = 1, 2, \ldots, s$) est une image de $M/(\overline{M}+M^*)$. Donc, on a, de la même manière que précédemment, le

Théorème 3: Le $\Gamma_{\overline{K}}$-rang de $M/\overline{M}$ ne dépasse pas celui de μ.

§ 3. Structure du groupe $\overline{Z}$. Nombres π et ρ normés. Facteurs de Rella. Anneaux $\overline{\Gamma}$ et $\overline{\Gamma}_k$.

On sait que le groupe Z est engendré par un élément $\overline{z}$, correspondant d'un élément z de Z tel que, pour tout $\alpha \in \Omega(K)$, on ait $z\alpha = \alpha^{\bar{\omega}}$, et par un élément $\overline{t}$, correspondant d'un élément t de T tel que, pour tout $\alpha \in K$ et d'ordre 1 pour $\mathfrak{P}$, $\frac{t\alpha}{\alpha}$ appartienne à l'exposant h (mod $\mathfrak{P}$). $\overline{z}^f$ appartient à $\overline{T}$, donc est de la forme $\overline{t}^a$. On peut choisir $\overline{t}$ de manière que $a \mid h$. Supposons qu'on ait fait un tel choix de $\overline{t}$ et posons $h = a\delta$. Alors, manifestement, $f\delta$ est l'ordre de $\overline{z}$.

Choisissons, d'une manière provisoire, un $\pi' \in K$ tel que $\omega(\pi') = 1$ et une racine primitive $\widetilde{\Omega} - 1^{ième}$ de l'unité ρ'. Définissons l'entier, pris (mod $\widetilde{\Omega} - 1 = p^F - 1$), $c(\pi', \rho')$ par l'égalité

$$\frac{z\pi'}{\pi'} \equiv \rho'^{\,c(\pi', \rho')} \pmod{\mathfrak{P}}.$$

Alors on a le

Théorème 4: $\delta = \dfrac{\bar{\omega} - 1}{[\bar{\omega} - 1,\ c(\pi', \rho')]}$ et $\delta \mid [\bar{\omega} - 1,\ h]$.

Démonstration: Posons $c(\pi', p') = c$. Alors, pour tout entier $a \geqslant 1$, on a

$$\frac{z^a\pi'}{\pi'} = z\left(\frac{z^{a-1}\pi'}{\pi'}\right).\ \frac{z\pi'}{\pi'} \equiv \left(\frac{z^{a-1}\pi'}{\pi'}\right)^{\bar\omega} \rho'^c \pmod{\mathfrak{P}}.$$

Or, la fonction $\psi(a) = \rho'^{c\frac{\bar\omega^a-1}{\bar\omega-1}}$ satisfait aux conditions $\psi(0)=1$ et

$$\psi(a) = \rho'^{c\frac{\bar\omega^a-1}{\bar\omega-1}} = \rho'^c.\ \rho'^{c\frac{\bar\omega^a-\bar\omega}{\bar\omega-1}} = \rho'^c.\ \psi(a-1)^{\bar\omega} \quad (a \geqslant 1).$$

Donc

$$\frac{z^a\pi'}{\pi'} \equiv \psi(a) \pmod{\mathfrak{P}} \quad (a = 0, 1, 2, \dots).$$

En particulier,

$$\frac{z^f\pi'}{\pi'} \equiv \psi(f) \equiv \rho'^{c\frac{\bar\omega^f-1}{\bar\omega-1}} \equiv \rho'^{c\frac{\widetilde{\Omega}-1}{\bar\omega-1}}.$$

Donc, puisque ρ' est une racine $\bar\omega-1$-ième primitive de l'unité, on a $\delta = \frac{\bar\omega-1}{[\bar\omega-1, c]}$. Donc $\delta|\bar\omega-1$. Comme $\delta|h$, on a $\delta\,|\,[\bar\omega-1, h]$, et tout est prouvé. Posons $\bar\omega-1 = \delta\Delta$. Alors on a le.

Théorème 5: *On peut choisir un $\pi \in K$ d'ordre 1 en $\mathfrak{P}$ et une racine primitive $\overline{\Omega}-1$-ième de l'unité ρ tels que $c(\pi,\rho) = \Delta$.*

Démonstration: Posons $\rho^a = \rho'$ avec un a premier à $\widetilde{\Omega}-1$, et $\pi = \rho'^b\pi'$ Montrons que a et b peuvent être choisis de manière que $c(\pi,\rho) = \Delta$. En effet

$$\frac{z\pi}{\pi} = \left(\frac{z\rho'}{\rho'}\right)^b.\frac{z\pi'}{\pi'} \equiv \rho'^{c(\pi',\rho')+(\bar\omega-1)b} \equiv \rho^{ac(\pi',\rho')+ab(\bar\omega-1)} \pmod{\mathfrak{P}},$$

donc

$$c(\pi,\rho) \equiv ac(\pi',\rho') + ab(\bar\omega-1) \pmod{\widetilde{\Omega}-1}.$$

Choisissons d'abord a de manière que

$$ac(\pi',\rho') \equiv \Delta \pmod{\widetilde{\Omega}-1}, \quad [a, \widetilde{\Omega}-1] = 1,$$

ce qui est possible parce que $[c(\pi',\rho'), \widetilde{\Omega}-1] = \Delta$. Ensuite choisissons b de manière que

$$ab \equiv -\frac{ac(\pi',\rho')-\Delta}{\bar\omega-1} \quad \left(\mathrm{mod}\ \frac{\widetilde{\Omega}-1}{\bar\omega-1} \equiv \frac{\bar\omega^f-1}{\bar\omega-1}\right),$$

ce qui est encore possible, parce que $[a, \widetilde{\Omega}-1] = 1$. On a alors

$$c(\pi,\rho) \equiv ac(\pi',\rho') + ab(\bar\omega-1) \equiv \Delta + (\bar\omega-1)\left[ab + \frac{ac(\pi',\rho')-\Delta}{\bar\omega-1}\right] \equiv$$

$$\equiv \Delta \pmod{\widetilde{\Omega}-1}.\ \text{C. q. f. d.}$$

Remarque: Il est à remarquer que $\bar z$ et $\bar t$ sont liés par la relation

$$\bar z\bar t = \bar t^{\bar\omega}\bar z;$$

ainsi le groupe $\bar Z$ est engendré par deux éléments $\bar z$, $\bar t$ liés par 3 relations, dont toute autre est une conséquence,

$$\bar t^h = 1, \quad \bar z^f = \overline{t^{\frac{h}{\delta}}}, \quad \bar z\bar t = \bar t^{\bar\omega}\bar z,$$

donc est défini, à isomorphisme près, par la donnée des 4 nombres f, h, δ, f_0, qui doivent satisfaire aux conditions $h|p^{f_0 f}-1$ et $\delta|[h, p^{f_0}-1]$. Considérons l'anneau $\bar\Gamma$. Soit $A(q)$ l'ensemble de tous les entiers q' qui satisfont, pour un entier s convenable, a la congruence

$$q' = qp^s \pmod{h}.$$

Soient $A_1, A_2, \dots, A_\mu$ toutes les $A(q)$ distincts. Alors on a la décomposition suivante de x^h-1 en facteurs irréductibles dans Ω_1:

$$x^h - 1 = \prod_{i=1}^{\mu} f_{A_i}(x),$$

où $f_{A_i}(x) = \prod_{q'}(x-\xi^{q'})$, ξ étant la racine h-ième primitive de l'unité dans $\Omega(K)$ égale au reste de $\frac{t\pi}{\pi}$, et q' parcourant l'ensemble complet des restes des nombres de A_i (mod h). Tous les $f_{A_i}(x)$ sont distincts et le dégré de $f_{A(q)}(x)$ est égal à l'exposant auquel appartient p (mod $\frac{h}{[h,q]}$) (donc, en particulier, ce dégré divise F). $f_{A(q)}(x)$ s'appellera le *q-facteur de Rella de* (x^h-1) [11].

Soit e_i un polynome en $\bar t$ dans Ω_1 satisfaisant aux conditions

$$\begin{cases} e_i \equiv 1 \pmod{f_{A_i}(\bar t)} \\ e_i \equiv 0 \pmod{f_{A_j}(\bar t)}, \text{ si } 1 \leqslant j \leqslant \mu \text{ et si } j \neq i. \end{cases}$$

e_i est un polynome en $\bar{t}$, soit $\varphi_i(\bar{t})$. Or $\bar{z}\,\bar{t}^j\,\bar{z}^{-1} = \bar{t}^{j\bar{\omega}}$. Donc $\bar{z}\,e_i\,\bar{z}^{-1} = \varphi_i(\bar{t}^{\bar{\omega}}) = \varphi_i(\bar{t})^{\bar{\omega}} = e_i^{\bar{\omega}}$. Donc

$$\bar{z}\,e_i\,\bar{z}^{-1} \equiv 0^{\bar{\omega}} \equiv 0 \pmod{f_{A_j}(\bar{t})}, \text{ si } j \neq i,$$

$$\bar{z}\,e_i\,\bar{z}^{-1} \equiv 1^{\bar{\omega}} \equiv 1 \pmod{f_{A_i}(\bar{t})},$$

c'est-à-dire $\bar{z}\,e_i\,\bar{z}^{-1} = e_i$ et e_i est permutable avec $\bar{z}$. Il l'est, manifestement, avec $\bar{t}$ et avec les éléments de l'anneau Ω_1, donc aussi avec tous les éléments de l'anneau $\bar{\Gamma}$ engendré par $\bar{z}$ et $\bar{t}$ sur Ω_1. Donc e_i appartient au centre de $\bar{\Gamma}$, et puisque $1 = e_1 + e_2 + \ldots\ldots + e_\mu$, $\bar{\Gamma}^{(A_i)} = e_i\,\bar{\Gamma} = \bar{\Gamma}\,e_i$ est un idéal bilatère de $\bar{\Gamma}$ et

$$\bar{\Gamma} = \bar{\Gamma}^{(A_1)} \oplus \bar{\Gamma}^{(A_2)} \oplus \ldots\ldots \oplus \bar{\Gamma}^{(A_\mu)}$$

est une décomposition directe de $\bar{\Gamma}$.

Un raisonnement absolument analogue peut se faire pour l'anneau $\bar{\Gamma}_k$. On n'a que remplacer les ensembles $A(q)$ par des ensembles $B(q)$ des entiers q' tels que, pour un s convenable,

$$q' \equiv q\,\bar{\omega}^s \pmod{h},$$

et Ω_1 par $\Omega(k) = \Omega_{f_0}$. $f_{B(q)}(x)$ sera $\prod_{q'}(x - \xi^{q'})$, où q' parcourt un ensemble complet de restes des nombres de $B(q) \pmod{h}$.

Il est visible que l'anneau $\bar{\Gamma}^{(A(q))}$ est isomorphe à l'anneau quotient de l'anneau $W_{f_0, \nu(q)}$, où $\nu(q)$ est le dégré de $f_{A(q)}(x)$, suivant son idéal bilatère $(z_{f_0}^f - \xi^{\frac{h}{\delta}q})$, où l'anneau $W_{a,b}$ est engendré sur Ω_b par un élément z_a satisfaisant aux seules relations.

$$z_a\,\alpha = \alpha^{p^a}\,z_a, \text{ pour tout } \alpha \in \Omega_b,$$

et à leurs conséquences. Cet isomorphisme se réalise par la correspondance

$$\bar{t} \to \xi^q,\ \bar{z} \to z_{f_0}.$$

Quant à $\bar{\Gamma}_k^{(B(q))}$, il est isomorphe à $W_{f_0, (f_0, \nu(q))} / (z_{f_0}^f - \xi^{\frac{h}{\delta}q})$.

Or, dans mon travail „Sur la primitivité des corps $\mathfrak{P}$-adiques" [17]), j'avais prouvé que tous les idéaux unilatéraux d'un $W_{a,b}$ sont principaux. Il en résulte que tous les idéaux de $\bar{\Gamma}$ ou de $\bar{\Gamma}_k$ le sont. En effet, soit $\bar{\gamma}$ un idéal à gauche, par exemple, de $\bar{\Gamma}$. Alors, si $\bar{\gamma}_i = e_i\,\bar{\gamma}$, on a

$$\bar{\gamma} = \bar{\gamma}_1 \oplus \bar{\gamma}_2 \oplus \ldots\ldots \oplus \bar{\gamma}_\mu .$$

Soit $\bar{\zeta}_i$ un élément de $\bar{\Gamma}^{(A_i)}$ tel que $\bar{\gamma}_i = \bar{\Gamma}^{(A_i)}\,\bar{\zeta}_i$. Alors, posons $\bar{\zeta} = \sum_{i=1}^{\mu} \bar{\zeta}_i$.

$$\bar{\zeta} \in \bar{\gamma} \quad \text{et} \quad \bar{\gamma} \ni e_i\,\bar{\zeta} = e_i \sum_{i=1}^{\mu} \bar{\zeta}_i = e_i\,\bar{\zeta}_i = \bar{\zeta}_i$$

(parce que $e_i^2 = e_i$, et si $\bar{\zeta}_i \in \Gamma^{(A_i)}$, donc $\bar{\zeta}_i = e_i\,\bar{\zeta}'$ ($\bar{\zeta}' \in \bar{\Gamma}$), on a $e_i = e_i^2\,\bar{\zeta}' = e_i\,\zeta' = \bar{\zeta}_i$); donc $\bar{\gamma} \supseteq \bar{\Gamma}\,\bar{\zeta} \supseteq \sum_{i=1}^{\mu} \bar{\gamma}_i = \bar{\gamma}$ et $\bar{\Gamma}\,\bar{\zeta} = \bar{\gamma}$.

c. q. f. d.

§ 4. Transformations $\bar{\zeta}^{(q)}$.

Considérons un nombre α de K et un élément $\zeta = \sum_{i=1}^{n} a_i\,\sigma_i$ ($a_i \in \mathfrak{S}_k$, $\sigma_i \in Z$) de Γ_k.

Supposons $\omega(\alpha) \geqslant q$ (q étant un entier rationnel quelconque.) Soit β la classe (mod $\mathfrak{P}$) à laquelle appartient $\frac{\alpha}{\pi^q}$. La classe (mod $\mathfrak{P}$) à laquelle appartient $\frac{\zeta\alpha}{\alpha}$ ne depend, manifestement, (pour ζ fixe) que de β. Pour un β fixe elle ne depend, d'autre part, que de l'élément $\bar{\zeta}$ de $\bar{\Gamma}_k$ correspondant de ζ. On désignera cette classe par $\bar{\zeta}^{(q)}\,\beta$. $\bar{\zeta}^{(q)}$ est donc une transformation de $\Omega(K)$.

---

[17]) Mathematica, t. XIII, 1937, p. 72-191[18]).

[18]) Je viens d'apprendre que les anneaux $W_{a,b}$ avaient été déjà considérés avant moi par M. Ore (Voir ses travaux des Annals of Math., 1933, t. 45, p. 480—508; Trans. of Amer. Math. Soc. t. 35, N. 3, p. 559-584. t. 36, N. 2, p. 8. 243-274).

On a $\overline{\zeta}^{(q)}(\beta_1+\beta_2)=\overline{\zeta}^{(q)}\beta_1+\overline{\zeta}^{(q)}\beta_2$; $(\overline{\zeta}_1+\overline{\zeta}_2)^{(q)}\beta=\overline{\zeta}_1^{(q)}\beta+\overline{\zeta}_2^{(q)}\beta$; $(\overline{\zeta}_1\overline{\zeta}_2)^{(q)}\beta=\overline{\zeta}_1^{(q)}(\overline{\zeta}_2^{(q)}\beta)$. Si $q>0$, et si $\omega(\alpha)\geqslant q$, on a (si $\zeta\in\Gamma$)

$$(1+\alpha)^{\zeta}=\prod_{i=1}^{n}(\sigma_i(1+\alpha))^{a_i}=\prod_{i=1}^{n}(1+\sigma_i\alpha)^{a_i}\equiv\prod_{i=1}^{n}(1+a_i.\sigma_i\alpha)\equiv$$

$$\equiv 1+\sum_{i=1}^{n}a_i.\sigma_i\alpha\equiv 1+\zeta\alpha\pmod{\mathfrak{P}^{q+1}}.$$

Donc

$$\frac{(1+\alpha)^{\zeta}-1}{\pi^q}\qquad\text{appartient à }\overline{\zeta}^{(q)}\beta.$$

Trouvons la forme explicite de la transformation $\overline{\zeta}^{(q)}\overline{t}^{(q)}\beta$ est la classe à laquelle appartient

$$\frac{t\alpha}{\pi^q}=t\left(\frac{\alpha}{\pi^q}\right)\left(\frac{t\pi}{\pi}\right)^q.\quad\text{Or}\quad t\left(\frac{\alpha}{\pi^q}\right)\equiv\frac{\alpha}{\pi^q}\pmod{\mathfrak{P}}\text{ et }\frac{t\pi}{\pi}\equiv\xi_{\cdot}\pmod{\mathfrak{P}}.$$

Donc

$$\overline{t}^{(q)}\beta=\xi^q\beta,$$

$\overline{z}^{(q)}\beta$ est la classe (mod $\mathfrak{P}$) à laquelle appartient

$$\frac{z\alpha}{\pi^q}=z\left(\frac{\alpha}{\pi^q}\right)\left(\frac{z\pi}{\pi}\right)^q\equiv\left(\frac{\alpha}{\pi^q}\right)^{\tilde{\omega}}\rho^{\Delta q}\pmod{\mathfrak{P}}.$$

Donc, si l'on désigne la classe (mod $\mathfrak{P}$) à laquelle appartient ρ aussi par la même lettre, on a

$$\overline{z}^{(q)}\beta=\rho^{\Delta q}\beta^{\tilde{\omega}}.$$

Donc, si

$$\overline{\zeta}=\sum_{i=1}^{\frac{h}{\delta}}\sum_{j=1}^{f\delta}a_{ij}\,\overline{t}^{i}\,\overline{z}^{j}$$

($\overline{\zeta}$ peut être, et d'une seule manière, représenté sous cette forme) on a

$$\overline{\zeta}^{(q)}\beta=\sum_{i=1}^{\frac{h}{\delta}}\sum_{j=1}^{f\delta}a_{ij}\,\xi^{iq}\,\rho^{\Delta q}\,\frac{\tilde{\omega}^j-1}{\tilde{\omega}-1}\beta^{\tilde{\omega}^j}.$$

Remarquons, que si $\zeta\in\Gamma$, soit

$$\overline{\zeta}=\sum_{i=1}^{\frac{h}{\delta}}\sum_{j=1}^{f\delta}a_{ij}\,\overline{t}^{i}\,\overline{z}^{j}\quad(a_{ij}\in\Omega_1),$$

on a

$$\overline{\zeta}^{(qp^s)}\beta^{p^s}=\sum_{i=1}^{\frac{h}{\delta}}\sum_{j=1}^{f\delta}a_{ij}\,\xi^{iqp^s}\,\rho^{\Delta qp^s}\frac{\tilde{\omega}^j-1}{\tilde{\omega}-1}\beta^{p^s\tilde{\omega}^j}=$$

$$=\left(\sum_{i=1}^{\frac{h}{\delta}}\sum_{j=1}^{f\delta}a_{ij}\,\xi^{iq}\,\rho^{\Delta q}\,\frac{\tilde{\omega}^j-1}{\tilde{\omega}-1}\beta^{\tilde{\omega}^j}\right)^{p^s}=(\overline{\zeta}^{(q)}.\,\beta)^{p^s},$$

parce que $a_{ij}^{p^s}=a_{ij}$. Et, de même, si $\zeta\in\Gamma_k$, donc les a_{ij} sont $\in\Omega(k)$, on a

$$\overline{\zeta}^{(q\tilde{\omega}^s)}\beta^{\tilde{\omega}^s}=(\overline{\zeta}^{(q)}\beta)^{\tilde{\omega}^s}.$$

D'autre part, si $\zeta\in\Gamma_k$, et si m est un entier, $\frac{mh\Delta}{\tilde{\omega}-1}=m\frac{h}{\delta}$ est entier et on a

$$\overline{\zeta}^{(q+mh)}(\rho^{-\frac{mh\Delta}{\tilde{\omega}-1}}\beta)=\sum_{i=1}^{\frac{h}{\delta}}\sum_{j=1}^{f\delta}a_{ij}\,\xi^{i(q+mh)}\,\rho^{\Delta(q+mh)}\frac{\tilde{\omega}^j-1}{\tilde{\omega}-1};$$

$$\rho^{-\frac{mh\Delta}{\tilde{\omega}-1}\tilde{\omega}^j}\beta^{\tilde{\omega}^j}=\sum_{i=1}^{\frac{h}{\delta}}\sum_{j=1}^{f\delta}a_{ij}\,\xi^{iq}\,\rho^{\Delta q}\frac{\tilde{\omega}^j-1}{\tilde{\omega}-1}.\,\rho^{-\frac{mh\Delta}{\tilde{\omega}-1}}.\,\beta^{\tilde{\omega}^j}=$$

$$=\rho^{-\frac{mh\Delta}{\tilde{\omega}-1}}.\,\overline{\zeta}^{(q)}\beta.$$

Désignons par $\Omega(K)^{(q)}$ le module $\Omega(K)$ avec Γ comme anneau d'opérateurs, obtenu en posant

$$\zeta\alpha=\overline{\zeta}^{(q)}\alpha.\quad(\zeta\in\Gamma,\ \alpha\in\Omega(K)),$$

et par $\Omega(K)_k^{(q)}$ le même module avec Γ_k comme anneau d'opérateurs,

$\zeta\,\alpha$ ($\zeta \in \Gamma_k$, $\alpha \in \Gamma\,(K)$) étant défini par la même formule. Alors on a les théorèmes suivantes:

Théorème 6: *Si* $A_{(q_1)} = A_{(q_2)}$, $\Omega\,(K)^{(q_1)}$ *et* $\Omega\,(K)^{(q_2)}$ *sont* Γ*-isomorphes. Par exemple, si*

$$q_1 = q\,p^{s_1} + m_1\,h,\quad q_2 = q\,p^{s_2} + m_2\,h,$$

cette Γ*-isomorphie se réalise en faisant correspondre à l'élément* $\rho^{-\frac{m_1\,h\,\Delta}{\bar\omega - 1}\beta^{p^{s_1}}}$ *de* $\Omega\,(K)^{(q_1)}$ *l'élément* $\rho^{-\frac{m_2\,h\,\Delta}{\bar\omega - 1}\beta^{p^{s_2}}}$ *de* $\Omega\,(K)^{(q_2)}$.

Théorème 7: *Si* $B\,(q_1) = B\,(q_2)$, $\Omega\,(K)_k^{(q_1)}$ *et* $\Omega\,(K)_k^{(q_2)}$ *sont* Γ_k*-isomorphes. Si* $q_1 = q\,p^{\bar\omega^{s_1}} + m_1 h$ *et si* $q_2 = q\,p^{\bar\omega^{s_2}} + m_2 h$, *cette* Γ_k*-isomorphie se réalise par la correspondance de l'élément* $\rho^{-\frac{m_1\,h\,\Delta}{\bar\omega - 1}\beta^{\bar\omega^{s_1}}}$ *de* $\Omega\,(K)_k^{(q_1)}$ *avec l'élément* $\rho^{-\frac{m_2\,h\,\Delta}{\bar\omega - 1}\beta^{\bar\omega^{s_2}}}$ *de* $\Omega\,(K)_k^{(q_2)}$.

Donc, nous pouvons faire correspondre à chaque classe A_i (c'est à-dire à chaque facteur de Rella) et à chaque classe B_i un module abstrait, respectivement avec Γ et Γ_k comme anneau d'opérateurs, défini à un opérateur-isomorphisme près et désigné respectivement par $\Omega\,(K)^{(A_i)}$, $\Omega\,(K)_k^{(B_i)}$, à savoir un module opérateur-isomorphe à un quelconque des modules. $\Omega\,(K)^{(q)}$ ou $\Omega\,(K)_k^{(q)}$, pour $q \in A_i$ resp. B_i. Il est à remarquer que $\zeta\,\alpha$ ($\alpha \in \Omega\,(K)^{(A_i)}$, $\zeta \in \Gamma$) ne depend que de la composante $\overline{\zeta}\,(A_i)$ de ζ dans $\overline{\Gamma}^{(A_i)}$. En effet, si $q \in A_i$ et si $j \neq i$,

$$e_j\,\overline{(i)}^{(q)}\,\beta = e_j\,(\xi^q)\,\beta = 0.$$

Donc, aussi, quelque soit $\zeta \in \Gamma$,

$$(\overline{\zeta}\,e_j)^{(q)}\,\beta = \overline{\zeta}^{(q)}\,(e_j^{(q)}\,\beta) = \overline{\zeta}^{(q)}\,0 = 0.$$

De même $\zeta\,\alpha$ ($\zeta \in \Gamma_k$, $\alpha \in \Omega\,(K)_k^{(B_i)}$) ne depend que de la composante $\overline{\zeta}\,(B_i)$ de $\overline{\zeta}$ dans $\overline{\Gamma}_k^{(B_i)}$.

Considérons le Γ-groupe $\mathfrak{U}/\overline{\mathfrak{U}}$ du § 2. On a $\mathfrak{U}_q = \mathfrak{U}_q\,\overline{\mathfrak{U}}\,\mathfrak{U}^*/\mathfrak{U}_{q+1}\,\overline{\mathfrak{U}}\,\mathfrak{U}^* = \mathfrak{U}_q\,\overline{\mathfrak{U}}\,\mathfrak{U}^*/(R_{q+1}\,\overline{\mathfrak{U}}\,\mathfrak{U}^* \cap \mathfrak{U}_q\,\overline{\mathfrak{U}}\,\mathfrak{U}^*) \simeq \mathfrak{U}_q\,\overline{\mathfrak{U}}\,\mathfrak{U}^*.\ R_{q+1}\,\overline{\mathfrak{U}}\,\mathfrak{U}^*/R_{q+1}\,\overline{\mathfrak{U}}\,\mathfrak{U}^* = \mathfrak{U}_q\,R_{q+1}$.

$R_{q+1}\,\overline{\mathfrak{U}}\,\mathfrak{U}^*/R_{q+1}\,\overline{\mathfrak{U}}\,\mathfrak{U}^* \simeq \mathfrak{U}_q\,R_{q+1}/(\mathfrak{U}_q\,R_{q+1} \cap \overline{\mathfrak{U}}\,\mathfrak{U}^*\,R_{q+1}) = \mathfrak{U}_q\,R_{q+1}/(\overline{\mathfrak{U}}\,\mathfrak{U}^*)_q\,R_{q+1}$, parce que $\mathfrak{U}_q \cap \overline{\mathfrak{U}}\,\mathfrak{U}^* = \mathfrak{U} \cap R_q \cap \overline{\mathfrak{U}}\,\mathfrak{U}^* = R_q \cap \overline{\mathfrak{U}}\,\mathfrak{U}^*$. Les isomorphismes intervenant dans ce calcul sont des Γ-isomorphismes, parce que $R_{q+1}\,\overline{\mathfrak{U}}\,\mathfrak{U}^*$ et $(\overline{\mathfrak{U}}\,\mathfrak{U}^*)_q\,R_{q+1}$ sont des Γ-groupes. On prouve de la même manière que pour le $\Gamma_{\overline{K}}$-module $M/\overline{M}$ considéré au § 2, $M_q + \mathfrak{P}^{q+1}/(\overline{M} + M^*)_q + \mathfrak{P}^{q+1}$ est $\Gamma_{\overline{K}}$-isomorphe à μ_q. On posera d'ailleurs, à partir d'ici, $\overline{K} = k$. Or $\mathfrak{U}_q\,R_{q+1}/(\overline{\mathfrak{U}}\,\mathfrak{U}^*)_q\,R_{q+1} \simeq (\mathfrak{U}_q\,R_{q+1}/R_{q+1})/((\overline{\mathfrak{U}}\,\mathfrak{U}^*)_q\,R_{q+1}/R_{q+1})$ (c'est encore une Γ-isomorphie). $\mathfrak{U}_q\,R_{q+1}/R_{q+1}$ est Γ-isomorphe à un sous-Γ-module P_q de $\Omega\,(K)^{(q)}$, et $(\overline{\mathfrak{U}}\,\mathfrak{U}^*)_q\,R_{q+1}/R_{q+1}$ l' est à un autre sous-Γ-module $\overline{P}_q$ de $\Omega\,(K)^{(q)}$ (et de P_q), l'isomorphie se réalisant par la correspondance

$$\varepsilon \to \frac{\varepsilon - 1}{\pi^q} + \mathfrak{P}$$

des éléments ε de $\mathfrak{U}_q\,R_{q+1}$ avec des éléments de $\Omega\,(K)$. Donc

$$U \simeq \bigoplus_{1 \leqslant j \leqslant s} P_{q_j}/\overline{P}_{q_j}.$$

De même $\mu_q \simeq ((M_q + \mathfrak{P}^{q+1})/\mathfrak{P}^{q+1})/(((\overline{M} + M^*)_q + \mathfrak{P}^{q+1})/\mathfrak{P}^{q+1})$ (l'isomorphie étant une Γ_k-isomorphie). Et $(M_q + \mathfrak{P}^{q+1})/\mathfrak{P}^{q+1}$ est Γ_k-isomorphe à un sous-Γ_k-module Q_q de $\Omega\,(K)_k^{(q)}$, et, de même, $((\overline{M} + M^*)_q + \mathfrak{P}^{q+1})/\mathfrak{P}^{q+1}$ l'est à un sous-Γ_k module $\overline{Q}_q$ de Q_q. On a encore

$$\mu \simeq \bigoplus_{1 \leqslant j \leqslant s} Q_{q_j}/\overline{Q}_{q_j}.$$

Considérons tous les q_j qui appartiennent à une classe A_i resp. B_i donnée. Soient

$$P^{(A_i)} = \bigoplus_{q_j \in A_i} P_{q_j},\quad \overline{P}^{(A_i)} = \bigoplus_{q_j \in A_i} \overline{P}_{q_j}$$

et respectivement

$$Q^{(B_i)} = \bigoplus_{q_j \in B_i} Q_{q_j},\quad \overline{Q}^{(B_i)} = \bigoplus_{q_j \in B_i} \overline{Q}_{q_j}.$$

Alors, manifestement, $\bigoplus_{1 \leqslant j \leqslant s} P_{q_j}/\overline{P}_{q_j}$ est la somme directe étendue à tous

les A_i des $P^{(A_i)}/\overline{P}^{(A_i)}$. De même $\bigoplus_{1 \leqslant j \leqslant s} Q_{q_j}/\overline{Q}_{q_j}$ est la somme directe étendue à tous les B_i des $Q^{(B_i)}/\overline{Q}^{(B_i)}$. On appellera A_i-*rang de* $\mathfrak{U}/\overline{\mathfrak{U}}$ le Γ-rang de $P^{(A_i)}/\overline{P}^{(A_i)}$ et, de même, on appellera B_i-rang de $M/\overline{M}$ le Γ_k-rang de $Q^{(B_i)}/\overline{Q}^{(B_i)}$. On a les

Théorème 8: Le Γ-rang de U est égal au maximum des A_i-rangs de $\mathfrak{U}/\overline{\mathfrak{U}}$; donc le Γ-rang de $\mathfrak{U}/\overline{\mathfrak{U}}$ ne dépasse pas le maximum des A_i-rangs de $\mathfrak{U}/\overline{\mathfrak{U}}$, et

Théorème 9: Le Γ_k-rang de μ est égal au maximum des B_i-rangs de $M/\overline{M}$; donc le Γ_k-rang de $M/\overline{M}$ ne dépasse pas le maximum de ses B_i-rangs.

Démonstration: La démonstration de deux théorèmes étant semblable, démontrons le premier: soit m le maximum de A_i-rang de $\mathfrak{U}/\overline{\mathfrak{U}}$. Il existe donc, pour chaque classe A_i, $m_i \leqslant m$ éléments de $P^{(A_i)}/\overline{P}^{(A_i)}$, soient $\alpha_1^{(i)}, \alpha_2^{(i)}, \ldots, \alpha_{m_i}^{(i)}$ tels que $P^{(A_i)}/\overline{P}^{(A_i)} = \sum_{j=1}^{m_i} \Gamma\, \alpha_j^{(i)}$. Posons, de plus, $\alpha_{m_i+1}^{(i)} = \alpha_{m_i+2}^{(i)} = \ldots = \alpha_m^{(i)} = 0$. On a encore $P^{(A_i)}/\overline{P}^{(A_i)} = \sum_{j=1}^{m} \Gamma\, \alpha_j^{(i)}$. Posons $\alpha_j = \bigoplus_i \alpha_j^{(i)}$ ($j = 1, 2, \ldots, m$, la somme directe est étendue à tous les A_i). On a $e_{i'}\, \alpha_j^{(i)} = \alpha_j^{(i)}$ ou 0 suivant que $i' = i$ ou $i' \neq i$. Donc $e_i\, \alpha_j = \alpha_j^{(i)}$. Donc $\Gamma\, \alpha_j \supseteq \sum_i \Gamma\, \alpha_j^{(i)} = \bigoplus_i \Gamma\, \alpha_j^{(i)}$. Donc $\sum_{j=1}^{m} \Gamma\, \alpha_j \supseteq \sum_{j=1}^{m} \bigoplus_i \Gamma\, \alpha_j^{(i)} = \bigoplus_i \sum_{j=1}^{m} \Gamma\, \alpha_j^{(i)} = \bigoplus_i P^{(A_i)}/\overline{P}^{(A_i)}$, et le Γ-rang de cette somme directe, Γ-isomorphe à U, est m. Le reste du théorème est évident.

§ 5. Théorème de Deuring et ses conséquences.

Maintenant nous allons nous occuper de la représentation exponentielle dans le groupe entier des 1-unités de K, c'est-à-dire nous prendrons pour $\mathfrak{U}$ ce groupe. Le groupe $\overline{\mathfrak{U}}$ sera constitué par le seul élément 1 ou, exceptionnellement, sera le groupe de toutes les racines de l'unité contenues dans $\mathfrak{U}$ dont les dégrés sont des puissances de p. Nous commencerons par nous occuper du cas où le corps K/k est sans ramifications supérieures (c'est-à-dire $V = \{1_K\}$, où 1_K est l'isomorphisme identique de K, ou, ce qui est la même chose, $e = h$). Ce cas constitue le premier et, d'ailleurs, le plus difficile chaînon d'un procédé inductif servant à résoudre ce problème. Corrélativement, nous nous occuperons aussi de quelques quéstions relatives à la représentation factorielle des Γ- et des Γ_k-modules.

M. Deuring[19]) a démontré un théorème dont un cas particulier, à savoir celui relatif aux champs de Galois,[20]) servira de base à notre recherche. Voici l'énoncé du théorème général de M. Deuring:

Théorème: *k étant un corps et K étant une extension galoisienne sèparable de dégré fint de k, il existe une base de K par rapport à k (dite base normale) formée des conjugués par rapport à k d'un de ses éléments.*

En particulier, si k est un champ de Galois $\overline{\Omega}$ de $\overline{\omega}$ éléments, donc K est aussi un champ de Galois Ω de $\omega = \overline{\omega}^{\nu}$ éléments, le groupe de $\Omega/\overline{\Omega}$ est la période d'un opérateur δ défini par la formule $\delta\alpha = \alpha^{\overline{\omega}}$ (pour tout $\alpha \in \Omega$). Donc, dans ce cas le théorème de Deuring se formule ainsi:

Il existe un $\alpha_0 \in \Omega$ tel que tout autre $\alpha \in \Omega$ peut se mettre sous la forme $\alpha = \varphi(\delta)\,\alpha_0$, $\varphi(x)$ étant un polynome à coefficients dans $\overline{\Omega}$.

Voici une démonstration élémentaire de cette proposition: Soit $\alpha \in \Omega$. L'ensemble de tous les polynomes $\varphi(x)$ (dans $\overline{\Omega}$) tels que $\varphi(\delta)\,\alpha = 0$ est un idéal de $\overline{\Omega}[x]$. Tous les idéaux de $\overline{\Omega}[x]$ étant principaux, il existe un polynome $\varphi_\alpha(x)$, défini à un facteur constant de $\overline{\Omega}$ près, tel que $\varphi(\delta)\,\alpha = 0$ soit équivalent à $\varphi_\alpha(x) \mid \varphi(x)$. On a, pour tout $\alpha \in \Omega$, $(\delta^{\nu} - 1)\,\alpha = \alpha^{\overline{\omega}^{\nu}} - \alpha = \alpha^{\omega} - \alpha = 0$. Donc $\varphi_\alpha(x) \mid x^{\nu} - 1$. Supposons qu'il n'existe aucun $\alpha \in \Omega$ tel que $\varphi_\alpha(x) = x^{\nu} - 1$. Soient $\varphi_{\alpha_1}(x) = \prod_{i=1}^{\lambda} f_i(x)^{\tau_i'}$, $\varphi_{\alpha_2}(x) = \prod_{i=1}^{\lambda} f_i(x)^{\tau_i''}$ les décomposttions de $\varphi_{\alpha_1}(x)$ et de $\varphi_{\alpha_2}(x)$ en facteurs premiers, où on a écrit tous les facteurs qui entrent dans un au moins de ces polynomes, en faisant, au besoin, $\tau_i' = 0$ ou $\tau_i'' = 0$. Soient

[19]) Math. Annalen, 1932-1933, t. 107, p. 140-144.

[20]) Ce cas parficulier avait été prouvé déjà par M. Hensel en 1933 (Journ. f. d. reine u. ang. Math., t. 103, p. 230-237).

$$A(x) = \prod_{\substack{1 \leqslant i \leqslant \lambda \\ \tau_i' \geqslant \tau_i''}} f_i(x)^{\tau_i'}, \qquad B(x) = \prod_{\substack{1 \leqslant i \leqslant \lambda \\ \tau_i' < \tau_i''}} f_i(x)^{\tau_i''}.$$

$A(x)\,B(x)$ est le p. p. c. m. des $\varphi_{\alpha_1}(x)$ et $\varphi_{\alpha_2}(x)$. Posons $\alpha = B(\delta)\,\alpha_1 + A(\delta)\,\alpha_2$. On a, manifestement, $A(\delta)\,B(\delta)\,\alpha = 0$, donc $\varphi_\alpha(x) \mid A(x)\,B(x)$. D'autre part,

$$A(\delta)\,\alpha = A(\delta)\,B(\delta)\,\alpha_1 + A(\delta)^2\,\alpha_2 = \prod_{\substack{1 \leqslant i \leqslant \lambda \\ \tau_i' \geqslant \tau_i''}} f_i'(\delta)^{2\tau_i'}.\,\alpha_2.$$

Donc, pour que $\varphi(\delta)\,A(\delta)\,\alpha = 0$, il faut, puisque tous les $f_i(x)$ sont distincts, que $B(x) \mid \varphi(x)$ Donc $B(x) \mid \varphi_\alpha(x)$. De la même manière on voit que $A(x) \mid \varphi_\alpha(x)$. Donc, puisque $A(x)$ et $B(x)$ sont premiers entre eux, $A(x)\,B(x) \mid \varphi_\alpha(x)$ et $\varphi_\alpha(x) = A(x)\,B(x)$. Donc, si $\Phi(x)$ est le p. p. c. m. de tous les φ_α, pour $\alpha \in \Omega$, il existe des $\alpha \in \Omega$ tels que $\varphi_\alpha(x) = \Phi(x)$.

Or, si $\Phi(x) \neq x^\nu - 1$, son dégré μ est $< \nu$. Soit donc $\Phi(x) = x^\mu + a_1 x^{\mu-1} + \ldots + a_\mu$. Alors $\Phi(\delta)\,\alpha = 0$ signifie $\alpha^{\overline{\omega}^\mu} + a_1 \alpha^{\overline{\omega}^{\mu-1}} + \ldots + a_\mu = 0$. Mais il y a au plus $\overline{\omega}^\mu$ éléments de Ω qui peuvent satisfaire a cette condition, ce qui est absurde, puisque $\omega = \overline{\omega}^\nu > \overline{\omega}^\mu$. Donc il existe un $\alpha_0 \in \Omega$ tel que $\varphi_{\alpha_0}(x) = x^\nu - 1$. Donc $\varphi(\delta).\,\alpha_0$ parcourt $\overline{\omega}^\nu = \omega$ éléments distincts de Ω, c'est-à-dire Ω entier, quand $\varphi(x)$ parcourt $\overline{\Omega}[x]$, et tout est prouvé.

Revenons à la notation du § 1. Soit $\overline{\rho}$ une racine $(\tilde{\omega}^f - 1)\,\delta$-ième primitive de l'unité telle que $\overline{\rho}^\delta = \rho$, où ρ est l'élément normé de $\Omega(K)$ introduit dans ce §. Appliquons le théorème de Deuring au champ de Galois $\Omega/\Omega(k)$, où Ω est le champ de Galois obtenu par l'adjonction de $\overline{\rho}$ à $\Omega(K)$. Le nombre d'éléments de Ω est $\tilde{\omega}^{f\psi}$, où ψ est le plus petit entier tel que $\tilde{\omega}^{f\psi} \equiv 1 \pmod{(\tilde{\omega}^f - 1)\,\delta}$, c'est-à-dire

$$1 + \tilde{\omega}^f + \tilde{\omega}^{2f} + \ldots + \tilde{\omega}^{(\psi-1)f} \equiv 0 \pmod{\delta}.$$

Or, on a vu que $\delta \mid \tilde{\omega} - 1$; donc, à fortiori, $\tilde{\omega}^f \equiv 1 \pmod{\delta}$, et la condition précédente peut s'écrire

$$\psi \equiv 0 \pmod{\delta}.$$

Donc $\psi = \delta$ et $(\Omega : \Omega(K)) = \delta$. Il en résulte que tout $\alpha \in \Omega$ se met, et d'une

seule manière, sous la forme $\alpha = \sum_{i=1}^{\delta} \sigma_i \overline{\rho}^i$ $(\alpha_i \in \Omega(K))$. Soit z_{f_0} l'automorphisme $\alpha \to \alpha^{\tilde{\omega}}$ qui engendre le groupe de $\Omega/\Omega(k)$. On a

$$z_{f_0}\alpha = \Big(\sum_{i=1}^{\delta} \alpha_i \overline{\rho}^i\Big)^{\tilde{\omega}} = \sum_{i=1}^{\delta} \alpha_i^{\tilde{\omega}}\, \overline{\rho}^{i\tilde{\omega}} = \sum_{i=1}^{\delta} \alpha_i^{\tilde{\omega}}\, \overline{\rho}^{i(\tilde{\omega}-1)}.\,\overline{\rho}^i = \sum_{i=1}^{\delta} \alpha_i^{\tilde{\omega}}\, \rho^{i\Delta}\overline{\rho}^i =$$

$$= \sum_{i=1}^{\delta} z^{(i)}\alpha_i.\,\overline{\rho}^i,$$

où $z^{(i)}$ est la transformation $\alpha \to \alpha^{\tilde{\omega}}\,\rho^{i\Delta}$ de $\Omega(K)$, parce que $\overline{\rho}^{\tilde{\omega}-1} = \rho^{\frac{\tilde{\omega}-1}{\delta}} = \rho^\Delta$. Donc, si $f(x)$ est un polynome dans $\Omega(K)$,

$$f(z_{f_0})\,\alpha = \sum_{i=1}^{\delta} f(z^{(i)})\,\alpha_i.\,\overline{\rho}^i,$$

où, si $f(x) = \sum_{j=0}^{\mu} a_j x^j$, on pose $f(z^{(i)})\,\alpha_i = \sum_{j=0}^{\mu} a_j.(z^{(i)})^j\,\alpha_i$, et où $(z^{(i)})^j$ est défini par la formule de récurrence $(z^{(i)})^j\,\alpha = z^{(i)}((z^{(i)})^{j-1}\alpha)$, donc $(z^{(i)})^j\,\alpha = \alpha^{\tilde{\omega}^j}\,\rho^{i\Delta\frac{\tilde{\omega}^j-1}{\tilde{\omega}-1}}$.

En vertu du théorème de Deuring il est possible de choisir un $\alpha \in \Omega$ tel que tout $\beta \in \Omega$ puisse se mettre sous la forme $f(z_{f_0})\,\alpha$. Donc, si

$$\alpha = \sum_{i=1}^{\delta} \alpha_i \overline{\rho}^i \quad (\alpha_i \in \Omega(K)), \qquad \beta = \sum_{i=1}^{\delta} \beta_i \overline{\rho}^i \quad (\beta_i \in \Omega(K)),$$

on a $\beta_i = f(z^{(i)})\,\alpha_i$.

Donc on a le

Théorème 10: *Il est possible de choisir δ éléments de $\Omega(K)$, soient $\alpha_1, \alpha_2, \ldots, \alpha_\delta$, tels que, $\beta_1, \beta_2, \ldots, \beta_\delta$ étant δ éléments arbitraires de $\Omega(K)$, il existe un polynome $f(x)$ dans $\Omega(k)$, bien défini* (mod $x^f - 1$), *tel que l'on ait, pour tous les $i = 1, 2, \ldots, \delta$ à la fois, $\beta_i = f(z^{(i)})\,\alpha_i$.*

§ 6. — Caractères. Addition et multiplication des caractères.

Soit $B=\overline{\{\beta_1,\beta_2,\ldots,\beta_\delta\}}$[21]) un ensemble ordonné de δ élèments de $\Omega(K)$. Posons, pour tout $\zeta\in\Gamma_k$,

$$\chi_q^{(B)}(\zeta)=\rho^{\frac{q-\bar{q}}{\delta}}\cdot\bar{\zeta}^{(q)}\left(\rho^{-\frac{q-\bar{q}}{\delta}}\beta_{\bar{q}}\right),$$

où $\bar{q}$ est le plus petit reste positif de q (mod δ). $\chi_q^{(B)}(\zeta)$ sera appelé *q-iéme caractère de ζ de base B*. B sera dite *base de caractères*. $\chi_q^{(B)}(\zeta)$ ne depend, manifestement, que de $\bar{\zeta}$ et même, ne depend que de la composante de $\bar{\zeta}$ dans $\Gamma_k^{(B(q))}$. On le notera aussi $\chi_q^{(B)}(\bar{\zeta})$. Soit que

$$\bar{\zeta}=\sum_{i=1}^{h'}\sum_{j=1}^{f\delta}a_{ij}\bar{t}^i\bar{z}^j=\sum_{i=1}^{h'}\bar{t}^i f_i(\bar{z})$$

(cette représentation n'est possible que d'une seule manière), où $h'=\frac{h}{\delta}$ et où $f_i(x)=\sum_{j=1}^{f\delta}a_{ij}x^j$ est un polynome dans $\Omega(k)$. Alors, en vertu du § 4, on a

$$\chi_q^{(B)}(\zeta)=\rho^{\frac{q-\bar{q}}{\delta}}\sum_{i=1}^{h'}\sum_{j=1}^{f\delta}a_{ij}\xi^{iq}\rho^{\Delta q}\frac{\tilde{\omega}^{j-1}}{\tilde{\omega}-1}\left(\rho^{-\frac{q-\bar{q}}{\delta}}\beta_{\bar{q}}\right)^{\tilde{\omega}^j}=$$

$$=\sum_{i=1}^{h'}\left(\xi^{iq}\sum_{j=1}^{f\delta}a_{ij}\rho^{\Delta q}\frac{\tilde{\omega}^{j-1}}{\tilde{\omega}-1}-\frac{q-\bar{q}}{\delta}(\tilde{\omega}^j-1)\,\beta_{\bar{q}}^{\tilde{\omega}^j}\right)=$$

$$=\sum_{i=1}^{h'}\left(\xi^{iq}\sum_{j=1}^{f\delta}a_{ij}\rho^{\Delta\bar{q}}\frac{\tilde{\omega}^{j-1}}{\tilde{\omega}-1}\beta_{\bar{q}}^{\tilde{\omega}^j}\right)=\sum_{i=1}^{h'}\xi^{iq}\cdot f_i(z^{(\bar{q})})\beta_{\bar{q}}$$

parce que $\frac{\tilde{\omega}-1}{\delta}=\Delta$. On voit, par conséquent, que si $q\equiv q'\pmod h$, $\chi_q^{(B)}(\zeta)=\chi_{q'}^{(B)}(\zeta)$. L'ensemble ordonné $\overline{\{\chi_1^{(B)}(\zeta),\chi_2^{(B)}(\zeta),\ldots,\chi_h^{(B)}(\zeta)\}}$ s'appelera *caractéristique de ζ de base B* et sera noté $\chi_B(\zeta)$.

[21]) $\overline{\{\alpha_1,\alpha_2,\ldots,\alpha_s\}}$ désigne l'ensemble $\{\alpha_1,\alpha_2,\ldots,\alpha_s\}$ ordonné de manière que α_i soit son i-ième élément.

Théorème 11. *Il est possible de choisir une base de caractères de façon que quelque soit l'ensemble ordonné de h éléments de $\Omega(K)$, il existe un $\zeta\in\Gamma_k$ dont la caractéristique soit cet ensemble ordonné. Et, pour cette base, $\chi(\zeta_1)=\chi(\zeta_2)$ entraine $\bar{\zeta}_1=\bar{\zeta}_2$.*

Démonstration: Il suffit de prendre pour la base en quéstion l'ensemble $A=\overline{\{\alpha_1,\alpha_2,\ldots,\alpha_\delta\}}$ du théorème 10 du § 5. En effet, soit $B=\overline{\{\beta_1,\beta_2,\ldots,\beta_h\}}$ un ensemble ordonné quelconque de h éléments de $\Omega(K)$. Pour prouver qu'il existe un $\zeta\in\Gamma_k$ tel que $\chi_q^{(A)}(\zeta)=\beta_q$ pour tout $q=1,2,\ldots,h$, il suffit de montrer qu'il existe des polynomes $f_i(x)$ $(i=1,2,\ldots,h')$ tels que

$$\text{(I)}\qquad\sum_{i=1}^{h'}\xi^{iq}\cdot f_i(z^{(\bar{q})})\alpha_{\bar{q}}=\beta_q\qquad(q=1,2,\ldots,h).$$

La résolution du système (I) équivaut a la résolution succéssive de deux systèmes

$$\text{(II)}\qquad\sum_{i=1}^{h'}\xi^{iq}y_{i,\bar{q}}=\beta_q\ (q=1,2,\ldots,h);$$

$$\text{(III)}\qquad f_i(z^{(\bar{q})})\,\alpha_{\bar{q}}=y_{i,\bar{q}}\qquad(i=1,2,\ldots,h';\ \bar{q}=1,2,\ldots,\delta).$$

Le système (II) se décompose en δ systèmes indépendants (II_1, $\text{II}_2,\ldots,\text{II}_\delta$), où ($\text{II}_{\bar{q}}$) est le système linéaire

$$(\text{II}_{\bar{q}})\qquad\sum_{i=1}^{h'}\xi^{i(\bar{q}+s\delta)}y_{i,\bar{q}}=\beta_{\bar{q}+s\delta}\qquad(s=0,1,\ldots,h'-1)$$

ne contenant que h' inconnues $y_{i,\bar{q}}$. Le déterminant de ce système et le Vandermondien d'ordre h'

$$D_{\bar{q}}=\left|\xi^{i(\bar{q}+s\delta)}\right|_{\substack{i=1,2,\ldots,h'\\ s=0,1,\ldots,h'-1}}=\xi^{\bar{q}\sum_{i=1}^{h'}i}\left|(\xi^\delta)^{is}\right|_{\substack{i=1,2,\ldots,h'\\ s=0,1,\ldots,h'-1}}=$$

$$=\xi^{\bar{q}\frac{h'(h'-1)}{2}}\prod_{\substack{i=1,2,\ldots,h'\\ 1\leqq i'<i}}(\xi^{\delta i}-\xi^{\delta i'}).$$

Or, si $1 \leqslant i' < i \leqslant h'$, $\xi^{\delta i} - \xi^{\delta i'} = \xi^{\delta i'}(\xi^{\delta(i-i')} - 1) \neq 0$, parce que $0 < i - i' < h' = \frac{h}{\delta}$, donc $0 < \delta(i-i') < h$. Donc $D_{\overline{q}} \neq 0$ et le système $(\mathrm{II}_{\overline{q}})$ a une solution dans $\Omega(K)$. Il en est de même du système (II).

Les $y_{i,\overline{q}}$ $(i = 1, 2, \ldots, h'; \overline{q} = 1, 2, \ldots, \delta)$ étant supposés connus, le système (III) se décompose en h' systèmes indépendants $(\mathrm{III}_1), (\mathrm{III}_2), \ldots, (\mathrm{III}_{h'})$, où (III_i) est le système

$$(\mathrm{III}_i) \qquad f_i(z^{(\overline{q})})\, \alpha_{\overline{q}} = y_{i,\overline{q}} \qquad (q = 1, 2, \ldots, \delta).$$

Le théorème 10 de § 5 montre que, quelques soient les $y_{i,\overline{q}} \in \Omega(K)$ $(q = 1, 2, \ldots, \delta)$, ce système est résoluble. Il en est donc de même pour le système (III) et pour le système (I), ce qui prouve la première partie du théorème. Le nombre d'éléments de $\overline{\Gamma}_k$ est $(\bar{\omega}^{f\delta})^{h'} = \bar{\omega}^{f\delta h'} = \bar{\omega}^{fh}$. Le nombre de leurs caractéristiques distinctes de base A est $(\bar{\omega}^f)^h = \bar{\omega}^{fh}$, c'est-à-dire le même. Donc deux éléments distincts de $\overline{\Gamma}_k$ ne peuvent pas avoir leurs caractéristiques (de base A) égales et tout est prouvé. On tire du théorème qui précède les conséquences suivantes;

1°) *si $\nu(B_i)$ est le dégré du facteur $f_{B_i}(x)$ de $x^h - 1$, le rang de la somme directe $P^{(B_i)}$ de $\nu(B_i)$ ensembles égaux à $\Omega(K)_k^{(B_i)}$ est* 1; en effet, il y a exactement $\nu(B_i)$ nombres q appartenant à B_i et tels que $0 < q \leqslant h$. Or, on a vu que si $\{\beta_q\}_{q \in B_i, 0 < q \leqslant h}$ est un ensemble quelconque d'éléments de $\Omega(K)$ il existe un $\zeta \in \Gamma_k$ tel que, pour tout $q \in B_i$ et tel que $0 < q \leqslant h$,

$$\zeta^{(q)}(\rho^{-\frac{q-\overline{q}}{\delta}}\, \alpha_{\overline{q}}) = \beta_q.$$

Remarquons que si $B_{(q_1)} = B_{(q_2)}$, on a $\overline{q_1} = \overline{q_2}$. En effet, on a alors $q_2 \equiv q_1\, \bar{\omega}^s \pmod{h}$ pour un s convenable. Or $q_1\, \bar{\omega}^s \equiv q_1 \pmod{\bar{\omega} - 1}$, donc $q_1 \equiv q_2 \pmod{\delta}$. Donc, si $q_1, q_2, \ldots, q_{\nu(B_i)}$ est l'ensemble de tous les $q \in B_i$ et tels que $0 < q \leqslant h$ (ils ont tous un même $\overline{q_i}$ qui sera noté $\overline{q}$),

$$\rho^{-\frac{q_1-\overline{q}}{\delta}}\, \alpha_{\overline{q}} \oplus \rho^{-\frac{q_2-\overline{q}}{\delta}}\, \alpha_{\overline{q}} \oplus \ldots\ldots\ldots \oplus \rho^{-\frac{q_{\nu(B_i)}-\overline{q}}{\delta}}\, \alpha_{\overline{q}}$$

est la base de

$$\Omega(K)_k^{(q_1)} \oplus \Omega(K)_k^{(q_2)} \oplus \ldots\ldots\ldots \oplus \Omega(K)_k^{(q_{\nu(B_i)})} \sim \bigoplus_{\nu(B_i)} \Omega(K)_k^{(B_i)}\ ^{22}),$$

ce qui prouve l'affirmation

2°) *Si $\alpha \in \Omega(k)$,*

$$\chi_q(\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_\delta)(\zeta) = \alpha\, \chi_q(\beta_1, \beta_2, \ldots, \beta_\delta)(\zeta).$$

Ceci résulte du fait que $\alpha^{\bar{\omega}} = \alpha$.

3°). *Soit $P^{(l)}$ la somme directe de $l\nu(A_i)$ ensembles égaux a $\Omega(K)^{(A_i)}$. Alors le rang de $P^{(l)}$ est lf_0.* En effet, d'abord le rang de $P^{(l)}$ ne dépasse pas l fois le rang de $P^{(1)}$. Or, soit $\{\gamma_1, \gamma_2, \ldots, \gamma_{f_0}\}$ une base de $\Omega(k)/\Omega_1$. Alors $\Gamma_k = \sum_{j=1}^{f_0} \gamma_j \Gamma$. Soient $B_{j_1}, B_{j_2}, \ldots, B_{j_\lambda}$ toutes les classes B_j contenues dans A_i. Dans tout $P^{(B_{j_u})}$ $(u = 1, 2, \ldots, \lambda)$ il existe, en vertu de 1°, un élément β_{j_u} tel que $\Gamma_k^{(B_{j_u})} \beta_{j_u} = P^{(B_{j_u})}$. D'autre part, si $u' \neq u$, $\Gamma_k^{(B_{j_{u'}})} \beta_{j_u} = \{0\}$. Donc

$$\Gamma_k(\beta_{j_1} \oplus \beta_{j_2} \oplus \ldots \oplus \beta_{j_\lambda}) = P^{(B_{j_1})} \oplus P^{(B_{j_2})} \oplus \ldots \oplus P^{(B_{j_\lambda})}.$$

Posons $\beta = \beta_{j_1} \oplus \beta_{j_2} \oplus \ldots \oplus \beta_{j_\lambda}$. Les opérateurs de $\Omega(K)_k^{(q)}$ et de $\Omega(K)^{(q)}$ désignés par un même $\zeta \in \Gamma$ étant les mêmes, on peut identifier $P^{(B_{j_1})} \oplus P^{(B_{j_2})} \oplus \ldots \oplus P^{(B_{j_\lambda})}$ avec $P^{(1)}$, et β sera alors identifié avec un élément de $P^{(1)}$, soit $\overline{\beta}$. On peut écrire

$$\Big(\sum_{j=1}^{f_0} \gamma_j \Gamma\Big)\beta = P^{(B_{j_1})} \oplus P^{(B_{j_2})} \oplus \ldots \oplus P^{(B_{j_\lambda})}.$$

Donc $\sum_{j=1}^{f_0} \Gamma.\, \gamma_j\, \overline{\beta} = P^{(1)}$, parce que, si $\beta_q \in \Omega(K)_k^{(q)}$,

$$\gamma_j \zeta.\, \beta_q = \rho^{-\frac{q-\overline{q}}{\delta}} \gamma_q (\rho^{\frac{q-\overline{q}}{\delta}} \beta_q)(\gamma_j \zeta) = \gamma_j \rho^{-\frac{q-\overline{q}}{\delta}} \gamma_q (\rho^{\frac{q-\overline{q}}{\delta}} \beta_q)(\zeta) = \gamma_j.\, \zeta\beta_q,$$

---

22) où $\bigoplus_m A$ désigne la somme directe de m modules égaux à A.

étant donné que $\gamma_j \in \Omega(k)$. Donc $\{\gamma_1\overline{\beta}, \gamma_2\overline{\beta}, \ldots, \gamma_{f_0}\overline{\beta}\}$ est une base de $P^{(1)}$ et le rang de $P^{(l)}$ ne dépasse pas lf_0.

Il ne peut pas être moindre, parce que $P^{(l)}$ a

$$(p^{ff_0})^{l\nu(A_i)} = (p^{f\nu(A_i)})^{lf_0}$$

éléments. Et comme $\overline{\Gamma}^{(A_i)}$ a $p^{f\nu(A_i)}$ éléments, $\Gamma\alpha = \overline{\Gamma}^{(A_i)}\alpha$ en a au plus autant, quelque soit $\alpha \in P^{(l)}$. Donc, si r est le rang de $P^{(l)}$ et si $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ en est une base,

$$\Gamma\alpha_1 + \Gamma\alpha_2 + \ldots + \Gamma\alpha_r = P^{(l)}$$

a au plus $(p^{f\nu(A_i)})^r$ éléments, donc $r \geqq lf_0$, ce qui achève la démonstration.

Théorème 12: a) *Si* $\alpha \in \Omega(k)$, $\chi_B(\alpha\zeta) = \alpha\,\chi_B(\zeta)$;

b) $\chi_B(\zeta_1 \pm \zeta_2) = \chi_B(\zeta_1) \pm \chi_B(\zeta_2)$.

Démonstration: C'est évident.

Theoreme 13: *Si* $f(x)$ *est un polynome dans* $\Omega(k)$ *et si* $\alpha = f(z^{\overline{(q)}})\,\alpha_{\overline{q}}$, $\rho^{\frac{q-\overline{q}}{\delta}}\zeta^{(q)}(\rho^{-\frac{q-\overline{q}}{\delta}}\alpha)$ *s'obtient en remplaçant dans l'expréssion de* $f(x)$ *chaque puissance* x^i *par* $(z^{\overline{(q)}})^i\,\chi^{(A)}_{q^{(i)}}(\zeta)$, *où* $q^{(i)}\bar{\omega}^i \equiv q \pmod h$.

Démonstration: En vertu du théorème précédent il suffit de prouver ce théorème en supposant $f(x) = x^i$, c'est-à-dire

$$\alpha = (z^{\overline{(q)}})^i\,\alpha_{\overline{q}} = \rho^{\overline{q}\,\Delta\frac{\bar{\omega}^i - 1}{\bar{\omega} - 1}}\alpha_{\overline{q}}^{\bar{\omega}^i}.$$

Donc

$$\rho^{-\frac{q-\overline{q}}{\delta}}\alpha = \rho^{-\frac{q-\overline{q}\,\bar{\omega}^i}{\delta}}\alpha_{\overline{q}}^{\bar{\omega}^i} = \rho^{-\frac{q-q^{(i)}\bar{\omega}^i}{\delta}}(\rho^{-\frac{q^{(i)}-\overline{q}}{\delta}}\alpha_{\overline{q}})^{\bar{\omega}^i}.$$

Donc

$$\rho^{\frac{q-\overline{q}}{\delta}}\zeta^{(q)}\left(\rho^{-\frac{q-\overline{q}}{\delta}}\alpha\right) = \rho^{\frac{q-\overline{q}}{\delta}}\cdot\rho^{-\frac{q-q^{(i)}\bar{\omega}^i}{\delta}}\left(\zeta^{(q^{(i)})}\left(\rho^{-\frac{q^{(i)}-\overline{q}}{\delta}}\alpha_{\overline{q}}\right)\right)^{\bar{\omega}^i} =$$

$$= \rho^{\frac{q-\overline{q}}{\delta} - \frac{q-q^{(i)}\bar{\omega}^i}{\delta}}\cdot\left(\rho^{-\frac{q^{(i)}-\overline{q}}{\delta}}\chi^{(A)}_{q^{(i)}}(\zeta)\right)^{\bar{\omega}^i} =$$

$$= \rho^{\frac{q-\overline{q}}{\delta} - \frac{q-q^{(i)}\bar{\omega}^i}{\delta} - \frac{q^{(i)}\bar{\omega}^i - q\bar{\omega}^i}{\delta}}\left(\chi^{(A)}_{q^{(i)}}(\zeta)\right)^{\bar{\omega}^i} = \rho^{\overline{q}\frac{\bar{\omega}^i-1}{\delta}}\left(\chi^{(A)}_{q^{(i)}}(\zeta)\right)^{\bar{\omega}^i} =$$

$$= \rho^{\overline{q}\,\Delta\frac{\bar{\omega}^i-1}{\bar{\omega}-1}}\left(\chi^{(A)}_{q^{(i)}}(\zeta)\right)^{\bar{\omega}^i} = (z^{\overline{(q)}})^i\,\chi^{(A)}_{q^{(i)}}(\zeta). \qquad \text{c. q. f. d.}$$

Théorème 14: *Si* $\chi^{(A)}_q(\zeta_2) = f(z^{\overline{(q)}})\,\alpha_{\overline{q}}$ (un tel $f(z^{\overline{(q)}})$ existe toujours en vertu du théorème 10 du § 5), $\chi^{(A)}_q(\zeta_1\zeta_2)$ *s'obtient en remplaçant dans* $f(x)$ *chaque terme* x^i *par* $(z^{\overline{(q)}})^i\,\chi^{(A)}_{q^{(i)}}(\zeta_1)$.

Démonstration: On a, en effet,

$$\chi^{(A)}_q(\zeta_1\zeta_2) = \rho^{\frac{q-\overline{q}}{\delta}}\cdot(\zeta_1\zeta_2)^{(q)}(\rho^{-\frac{q-\overline{q}}{\delta}}\alpha_{\overline{q}}) = \rho^{\frac{q-\overline{q}}{\delta}}\cdot$$

$$\zeta_1^{(q)}(\rho^{-\frac{q-\overline{q}}{\delta}}\cdot\rho^{\frac{q-\overline{q}}{\delta}}\zeta_2^{(q)}(\rho^{-\frac{q-\overline{q}}{\delta}}\alpha_{\overline{q}})) = \rho^{\frac{q-\overline{q}}{\delta}}\zeta_1^{(q)}(\rho^{-\frac{q-\overline{q}}{\delta}}\chi^{(A)}_q(\zeta_2)),$$

et on n'a que appliquer le théorème précédent.

On voit que $\chi^{(A)}_q(\zeta_1\zeta_2)$ ne depend que de $\chi^{(A)}_q(\zeta_2)$ et des seuls $\chi^{(A)}_{q'}(\zeta_1)$ tels que q' $(0 < q' \leqslant h)$ appartienne à $B(q)$. Nous dirons deux caractères $\chi^{(A)}_{q_1}(\zeta)$ et $\chi^{(A)}_{q_2}(\zeta)$ de ζ *conjugués par rapport à* k si $B(q_1) = B(q_2)$. Nous les dirons *conjugués absolus* si $A(q_1) = A(q_2)$. On voit que le q-ième caractère du produit ne depend que de caractères des facteurs conjugués par rapport à k du q-ième.

On pouvait, d'ailleurs, prévoir ce fait, parce que: 1^0) $\chi^{(A)}_q(\zeta)$ ne depend que de la composante de ζ dans $\Gamma^{(B_q)}_k$; 2^0) inversement, la donnée de tous les $\chi^{(A)}_q(\zeta)$, $q \in B_i$ et $0 < q \leqslant h$, définit la composante de $\overline{\zeta}$ dans $\overline{\Gamma}^{(B_i)}_k$; en effet, le nombre de systèmes distincts possibles de ces caractères est $\bar{\omega}^{f\nu(B_i)}$, c'est-à-dire est égal au nombre d'éléments de $\overline{\Gamma}^{(B_i)}_k$.

§ 7. — Théorème de Emmy Noether.

Emmy Noether avait démontré [23]) que l'anneau $\mathfrak{S}_K$ admet une base normale (c'est-à-dire formée par les conjugués par rapport à k d'un de ses éléments) par rapport a $\mathfrak{S}_k$, si, et seulement si le corps $\mathfrak{P}$-adique K/k est sans ramifications supérieures, c'est-à-dire si $e = h$. De ce qui précède découle une démonstration simple de ce théorème.

Lemme 2: *Si un* Γ_k*-module* M *de rang* $(K:k)$ *par rapport à* $\mathfrak{S}_k$ *admet une base normale par rapport à* $\mathfrak{S}_k$, *tout nombre de* $M \cap k$ *est la trace* (*de* K *à* k) *d'un nombre de* M.

Démonstration: Dans l'hypothèse de l'énoncé il existe un $\alpha \in M$ tel que $M = \Gamma_k\alpha$. Or $(\Gamma_k : \mathfrak{S}_k) = (K:k) = (M : \mathfrak{S}_k)$ [24]). Donc $\zeta\alpha = 0$ entraîne

[23]) Journ. f. d. reine u. ang. Math., 1931, t. 167, p. 147-152.

[24]) $(M : E_k)$ désigne le rang de M par rapport à E_k. Il n'est pas obligatoire que $M \geq E_k$!.

$\zeta = 0$. Or, si $\beta \in M \cap k$, on a, quelque soit $\sigma \in G_{K/k}$, $(\sigma - 1)\beta = 0$. Donc, si $\beta = \zeta_\beta \alpha, \zeta_\beta \in \Gamma_k$, on a, quelque soit $\sigma \in G_{K/k}$, $(\sigma - 1)\zeta_\beta = 0$. Soit $G_{K/k} = \{\sigma_1 = 1_k, \sigma_2, \ldots, \sigma_n\}$. Soit $\zeta_\beta = \sum_{i=1}^{n} a_i \sigma_i$ $(a_i \in \mathfrak{E}_k)$. Alors, quelque soit $j = 1,2,\ldots,n$, on a

$$0 = (\sigma_j^{-1} - 1) \sum_{i=1}^{n} a_i \sigma_i = (a_j - a_1) 1_K + \sum_{i=1}^{j-1} a_i \sigma_j^{-1} \sigma_i +$$

$$+ \sum_{i=j+1}^{n} a_i \sigma_j^{-1} \sigma_i - \sum_{i=2}^{n} a_i \sigma_i,$$

ce qui entraîne $a_j = a_1$. Donc tous les a_j, $j = 1, 2, \ldots, n$ sont égaux; soit a leur valeur commune. Alors

$\beta = a(\sigma_1 + \sigma_2 + \ldots + \sigma_n)\alpha = (\sigma_1 + \sigma_2 + \ldots + \sigma_n)(a\alpha) = S_{K/k}(a\alpha)$[25]. c. q. f. d.

Démonstration du théorème de Noether: Si e n'est pas premier à p, soit K_0/k le corps de ramification de K/k; on a $S_{K/k}\,\alpha = S_{K_0/k}(S_{K/K_0}\alpha)$. Or, si $\alpha \in \mathfrak{E}_K$, et si $\sigma \in G_{K/K_0} = V_{K/k}$, on a $\sigma\alpha \equiv \alpha \pmod{\mathfrak{P}}$. Donc, si $(K : K_0) = p^{\overline{\mu}}$, on a $S_{K/K_0}\,\alpha \equiv p^{\overline{\mu}}\alpha \equiv 0 \pmod{\mathfrak{P}}$. Donc aussi $S_{K_0/k}(S_{K/K_0}\alpha) \equiv 0 \pmod{\mathfrak{P}}$, parce que K/k est un corps $\mathfrak{P}$-adique. Donc $1 \in \mathfrak{E}_K \cap k$ ne peut pas être la trace de K à k d'un nombre de $\mathfrak{E}_K$. Donc $\mathfrak{E}_K$ n'admet pas de base normale par rapport à $\mathfrak{E}_k$.

Soit $e = h$. On a $\mathfrak{E}_K^* = \mathfrak{p}$. Donc, si $q < 0$ ou si $q \geqslant e = h$, on a $Q_q = \overline{Q}_q$. Si $0 \leqslant q < h$, on a $Q_q = \Omega(K)_k^{(q)}$ et $\overline{Q}_q = \{0\}$. Le nombre des q appartenant à une classe B_i et tels que $0 \leqslant q < h$ est $\nu(B_i)$. Donc $Q^{(B_i)}$ est la somme directe des $\nu(B_i)$ modules Γ_k-isomorphes à $\Omega(K)_k^{(B_i)}$ et $\overline{Q}^{(B_i)} = \bigoplus_{\nu(B_i)} \{0\}$. On a vu que le rang d'un tel module est 1. Donc tous les B_i-rangs de $\mathfrak{E}_K/\{1\}$ sont égaux à 1, et le Γ_k-rang de $\mathfrak{E}_K/\{1\}$ est aussi 1.

c. q. f. d.

[25]) $S_{K/k}(\alpha)$ désigne la trace de K à k du nombre α.

§ 8. Représentation exponentielle dans les corps sans ramifications supérieures.

Désignons par $\mathfrak{U}$ le groupe multiplicatif de toutes les 1-unités du corps $\mathfrak{P}$-adique galoisien K/k, supposé être sans ramifications supérieures. Prenons $\overline{\mathfrak{U}} = \{1\}$. $\mathfrak{U}^*$ est le groupe des puissances p-ièmes d'éléments de $\mathfrak{U}$. En vertu du théorème de Hensel, cité dans l'introduction:

a) $\overline{P}_q = \{0\}$ si $q \leqslant E\frac{p}{p-1}$ (où $E = ee_0$ est l'ordre absolu de $\mathfrak{P}$) et est premier à p; b) quand $E \equiv 0 \pmod{p-1}$, $\overline{P}_{E\frac{p}{p-1}} = \Omega(K)\left(E\frac{p}{p-1}\right)$ ou est un sous-module d'indice p de $\Omega(K)\left(E\frac{p}{p-1}\right)$ suivant que K est régulier (c'est-à-dire ne contient pas les racines p-ièmes primitives de l'unité) ou irrégulier (c'est-à-dire les contient); c) pour tous les autres q, $\overline{P}_q = \Omega(K)^{(q)}$. Quant à P_q, il est *toujours égal à* $\Omega(K)^{(q)}$.

Commençons par le cas régulier. Évaluons combien il se trouve des nombres q tels que $P_q \neq \overline{P}_q$ (c'est-à-dire $\overline{P}_q \neq \Omega(K)^{(q)}$) dans une classe A_i donnée? On peut remplacer chacun de ces nombres q par un autre nombre de la même classe sans que la distribution de ces nombres entre les classes change. Subdivisons l'intervalle $\left(0, E\frac{p}{p-1}\right)$ en intervalles successifs

$$\Delta_i = \left(E\frac{p^i - 1}{p^{i-1}(p-1)}, E\frac{p^{i+1} - 1}{p^i(p-1)}\right] \quad (i = 0, 1, \ldots, +\infty).$$

Désignons par $\overset{(i)}{q}$ chacun des q contenus dans l'intervalle Δ_i et tels que $\overline{P}_q \neq \Omega(K)^{(q)}$, c'est-à-dire chacun des q premiers à p et contenus dans Δ_i. Remplaçons chaque $\overset{(i)}{q}$ par

$$\overset{(i)}{q^*} = p^i \overset{(i)}{q} - E\frac{p(p^i - 1)}{p - 1} = \lambda^i(\overset{(i)}{q}),$$

où $\lambda(q)$ est la transformation $q \to p(q - E)$. Manifestement $\overset{(i)}{q^*} \in A(\overset{(i)}{q})$, parce que $\overset{(i)}{q^*} \equiv \overset{(i)}{q}\, p^i \pmod{E}$, donc aussi (mod h). Montrons que l'ensemble de tous les $\overset{(i)}{q^*}$ $(i = 0, 1, \ldots, +\infty)$ est l'ensemble de tous les entiers de l'intervalle $(0, E]$. En effet, premièrement

$$p^i . E\frac{p^i-1}{p^{i-1}(p-1)} - E\frac{p(p^i-1)}{p-1} < \overset{(i)}{q^*} \leqslant p^i . E\frac{p^{i+1}-1}{p^i(p-1)} - E\frac{p(p^i-1)}{p-1},$$

c'est-à-dire

$$0 < \overset{(i)}{q^*} \leqslant E;$$

deuxièmement, si $\overset{(i)}{q_1}^* = \overset{(j)}{q_2}^*$, on a

$$p^i \overset{(i)}{q_1} - p^j \overset{(j)}{q_2} = E\frac{p(p^i-1)}{p-1} - E\frac{p(p^j-1)}{p-1} = E\frac{p(p^i-p^j)}{p-1};$$

si $i \neq j$, étant donné que $\overset{(i)}{q_1}$ et $\overset{(i)}{q_2}$ sont premiers à p, l'ordre du premier membre de cette égalité pour p ne dépasse pas $\mathrm{Min}(i, j)$. Mais l'ordre du second membre pour p est au moins égal à $\mathrm{Min}(i, j)+1$. Ceci est absurde, donc $i=j$. Mais alors l'égalité devient $p^i \overset{(i)}{q_1} - p^i \overset{(i)}{q_2} = 0$, c'est-à-dire $\overset{(i)}{q_1} = \overset{(i)}{q_2}$. Donc tous les $\overset{(i)}{q^*}$ sont distincts et contenus dans l'intervalle $(0, E]$. Mais leur nombre, égal à celui des $\overset{(i)}{q}$, est

$$\left[E\frac{p}{p-1}\right] - \left[\frac{E\frac{p}{p-1}}{p}\right] = E + \left[\frac{E}{p-1}\right] - \left[\frac{E}{p-1}\right] = E,$$

et l'affirmation est prouvée. Étant donné que $E = e_0 e = e_0 h$, on voit que dans une classe A_i se trouvent $e_0 \nu(A_i)$ nombres q^*, donc aussi autant des q. Par conséquent, P^{A_i} est la somme directe de $e_0 \nu(A_i)$ Γ-modules Γ-isomorphes à $\Omega(K)^{(A_i)}$. Donc, puisque $\overline{P}^{(A_i)} = \{0\}$, on voit, en vertu du **§ 6**, que le A_i-rang de $\mathfrak{U}/\{1\}$ est $e_0 f_0 = n_0$, où n_0 est le dégré absolu de k. Donc, dans le cas régulier, le Γ-rang de $\mathfrak{U}/\{1\}$ ne dépasse pas n_0. Il ne peut pas aussi être plus petit, parce que alors le rang de $\mathfrak{U}/\mathfrak{U}^*$ ne dépasserait pas $(n_0 - 1)\, n = N - n < N$ (n-dégré de K/k, N-dégré absolu de K), parce que le groupe $\varepsilon^\Gamma/\varepsilon^{p\Gamma}$ est, au plus, de rang $(\Gamma : \mathfrak{S}) = n$; mais ce rang est N. Pour une raison semblable, si $\mathfrak{U} = \varepsilon_1^\Gamma \varepsilon_2^\Gamma \ldots \varepsilon_{n_0}^\Gamma$,

$$\varepsilon_1^{\zeta_1} \varepsilon_2^{\zeta_2} \ldots \varepsilon_{n_0}^{\zeta_{n_0}} = 1 \quad (\zeta_1, \zeta_2, \ldots, \zeta_{n_0} \in \Gamma)$$

ne peut avoir lieu que si $\zeta_1 = \zeta_2 = \ldots = \zeta_{n_0} = 0$, parce que autrement le rang en quéstion serait au plus $N-1$.

Si K est irrégulier, c'est-à-dire contient des racines p-ièmes primitives de l'unité, il est visible que l'analyse précédente s'applique à condition d'ajouter aux $\overset{(i)}{q}$ précédents encore le nombre $q_0 = E\frac{p}{p-1}$. Ceci ne change pas les résultats relatifs aux classes autres que $A(q_0) = A(\frac{E}{p-1})$; en ce qui concerne cette dernière classe, on voit que le $A(q_0)$-rang de $\mathfrak{U}/\{1\}$ ne depasse pas n_0+1. Donc le Γ-rang de $\mathfrak{U}/\{1\}$ ne depasse pas n_0+1. Il ne peut pas être moindre parce que alors le rang du groupe $\mathfrak{U}/\mathfrak{U}^*$ serait au plus $n_0\, n = N$, et l'on sait que dans le cas irrégulier il est $N+1$. Si $\varepsilon_1^\Gamma . \varepsilon_2^\Gamma \ldots \varepsilon_{n_0+1}^\Gamma = \mathfrak{U}$, il doit exister n rélations (R_i)

$$(R_i) \qquad \varepsilon_1^{\nu_1^{(i)}} \varepsilon_2^{\nu_2^{(i)}} \ldots \varepsilon_{n_0+1}^{\nu_{n_0+1}^{(i)}} = 1 \quad (i = 1, 2, \ldots, n)$$

telles que le système

$$\sum_{i=1}^{n} a_i \nu_j^{(i)} = 0 \qquad (j = 1, 2, \ldots, n_0+1)$$

n'ait d'autre solution dans $\mathfrak{S}$ que $a_1 = a_2 = \ldots = a_n = 0$ (on dit dans ce cas que les n relations sont linéairement indépendantes par rapport à $\mathfrak{S}$. Si le nombre des relations linéairement indépendantes par rapport à $\mathfrak{S}$ entre certaines 1-unités est nul, elles sont dites 1-unités indépendantes). En effet, le rang exponentiel infini de $\mathfrak{U}$ est N. On vient ainsi au

Théorème 15: *Si le surcorps K de k est galoisien, régulier et sans ramifications supérieures par rapport à k, le Γ-rang du groupe $\mathfrak{U}$ de ses 1-unités est n_0, et $\mathfrak{U}$ admet une Γ-base exponentielle formée de n_0 1-unités indépendantes. Si K/k est galoisien et sans ramifications supérieures, mais si K est irrégulier, le Γ-rang de $\mathfrak{U}$ est n_0+1, et les n_0+1 1-unités formant une Γ-base exponentielle de $\mathfrak{U}$ sont liées par n relations linéairement indépendantes par rapport à $\mathfrak{S}$.*

Démontrons encore le théorème suivant:

Théorème 16: *K/k étant galoisien et de dégré $(K:k)$ premier à p, et K étant irrégulier; $\mathfrak{U}$ désignant le groupe des 1-unités de K, et $\overline{\mathfrak{U}}$ étant le groupe de toutes les racines de l'unité contenues dans $\mathfrak{U}$; le Γ-rang de $\mathfrak{U}/\overline{\mathfrak{U}}$ est n_0 et $\mathfrak{U}/\overline{\mathfrak{U}}$ admet une Γ-base $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n_0}\}$ formée de 1-unités indépendantes et telles que $\varepsilon_1^\Gamma \varepsilon_2^\Gamma \ldots \varepsilon_{n_0}^\Gamma \cap \overline{\mathfrak{U}} = \{1\}$.*

Démonstration: Ce cas se distingue du cas des corps irréguliers du théorème précédent uniquement par ce que, p^v étant la contribution de p dans E, $P^{\frac{E}{p^v(p-1)}}$ n'est plus $\{0\}$, mais un Γ-module de p éléments.

Le raisonnement est absolument identique au précédent en ce qui concerne les classes A_i autres que $A(q_0)$, et on voit que pour ces classes le A_i-rang est n_0. En ce qui concerne $A(q_0)$, $P^{(A(q_0))}$ est, visiblement, la somme directe de e_0+1 modules Γ-isomorphes à $\Omega(K)^{(A(q_0))}$, parce que on a

$$q_0 p = \frac{Ep^2}{p-1} \equiv \frac{Ep}{p-1} \equiv q_0 \pmod{E}, \text{ donc } \pmod{h},$$

et, par conséquent, $\nu(A(q_0))=1$. Quant à $\overline{P}^{(A(q_0))}$, il est la somme directe de e_0-1 modules égaux à $\{0\}$, du module $\overline{P}_{\frac{E}{p^v(p-1)}}$ de p éléments, et du module $\overline{P}_{\frac{Ep}{p-1}}$ de $\frac{\omega f}{p}$ éléments. Le rang de $P^{(A(q_0))}/\overline{P}^{(A(q_0))}$ est, manifestement, égal à $(e_0-1)f_0 = n_0 - f_0$, augmenté du rang de

$$\Omega(K)^{\left(\frac{E}{p^v(p-1)}\right)} \oplus \Omega(K)^{\left(\frac{Ep}{p-1}\right)} / \overline{P}_{\frac{E}{p^v(p-1)}} \oplus \overline{P}_{\frac{Ep}{p-1}}.$$

Soit ε une 1-unité de K congrue à 1 $\left(\pmod{\mathfrak{P}^{\frac{E}{p^v(p-1)}}}\right)$. Soit $\alpha(\varepsilon)$ la classe (mod $\mathfrak{P}$) à laquelle appartient $\pi^{\frac{\varepsilon-1}{E}p^v(p-1)}$. On sait, d'après les travaux de M. Hensel, que $\varepsilon^{p^{v+1}} \equiv 1 \left(\pmod{\mathfrak{P}^{\frac{Ep}{p-1}} = \mathfrak{P}^{q_0}}\right)$, et que la classe (mod $\mathfrak{P}$) à laquelle appartient $\pi^{\frac{\varepsilon^{p^{v+1}}-1}{q_0}}$ ne depend que du $\alpha(\varepsilon)$. Désignons la par $\psi(\alpha(\varepsilon))$. On voit facilement que $\psi(\alpha_1+\alpha_2) = \psi(\alpha_1)+\psi(\alpha_2)$ et que, si $\sigma \in G_{K/k}$,

$$\psi\left(\sigma\left(\frac{E}{p^v(p-1)}\right)\alpha\right) = \sigma\left(\frac{Ep}{p-1}\right)\psi(\alpha)$$

(parce que $(\sigma\alpha)^{p^{v+1}} = \sigma_n^{\ast}\alpha^{p^{v+1}}$). Donc $\alpha \to \psi(\alpha)$ est un Γ-homomorphisme de $\Omega(K)^{\left(\frac{E}{p^v(p-1)}\right)}$ dans $\Omega(K)^{(q_0)}$. On sait que $\psi(\alpha)=0$ si, et seulement si $\alpha \in \overline{P}_{\frac{E}{p^v(p-1)}}$. Puisque $f_{A(q_0)}(z)$ est de dégré 1, $\Gamma^{(A(q_0))}$ est isomorphe

à l'anneau de restes des polynomes en z dans Ω_1 suivant l'idéal $(z^f - \xi^{q_0\frac{h}{\delta}})$[26]. Puisque nous avons supposé que $n=(K:k)$ est premier à p, f l'est aussi. Donc $(z^f - \xi^{q_0\frac{h}{\delta}})$ n'a aucun facteur premier double. En vertu du théorème de Deuring, il existe f_0 éléments de $\Omega(K)$, soient $\alpha_1, \alpha_2, \ldots, \alpha_{f_0}$, tels que

$$\Omega(K)^{\left(\frac{E}{p^v(p-1)}\right)} = \Gamma\alpha_1 + \Gamma\alpha_2 + \ldots + \Gamma\alpha_{f_0}.$$

Soit que

$$\psi(\alpha_i) = \sum_{j=1}^{f_0} \varphi_{ij}(z)\,\alpha_j.$$

Par la méthode bien connue on prouve que la base $\alpha_1, \alpha_2, \ldots, \alpha_{f_0}$ peut être choisie de manière que tous les $\varphi_{ij}(z)$ avec $j>i$ soient nuls. Alors, le nombre de classes de restes dans $\Omega(K)^{(q_0)}$ suivant le $\Gamma^{(A(q_0))}$-idéal

$$\Psi = (\psi(\alpha_1), \psi(\alpha_2), \ldots, \psi(\alpha_{f_0}),$$

égal a $\overline{P}_{q_0}$, est égal au produit des nombres n_i de classes de restes dans $\Omega_1[z]/(z^f - \xi^{q_0\frac{h}{\delta}})$ suivant

$$(\varphi_{ii}(z), z^f - \xi^{q_0\frac{h}{\delta}})/(z^f - \xi^{q_0\frac{h}{\delta}}) \quad (i=1,2,\ldots,f_0);$$

c'est-à-dire, si l_i est le dégré du p. g. c. d. des $\varphi_{ii}(z)$ et $z^f - \xi^{q_0\frac{h}{\delta}}$, ce nombre est $p^{\Sigma l_i}$. Or, étant donné que $\psi(\alpha)=0$ entraîne $\alpha \in \overline{P}_{\frac{E}{p^v(p-1)}}$, et que le nombre d'éléments de ce module est p, on voit que $(\Omega(K):\Psi)=p$. Donc $\sum_{i=1}^{f_0} l_i = 1$. Donc, on peut poser, en numérotant convenablement les α_i, $l_1=1$; $l_2=l_3=\ldots=l_{f_0}=0$. Soit que $(\varphi_{11}(z), z^f - \xi^{q_0\frac{h}{\delta}}) = \mathcal{P}_1(z^f - \xi^{q_0\frac{h}{\delta}}) = \mathcal{P}_1\mathcal{P}_2$. Cherchons la condition pour que α soit

[26]) En effet, le q_0-facteur de Rella est $t - \xi^{q_0}$.

dans $\overline{P}_{\frac{E}{p^v(p-1)}}$. Soit $\alpha = \sum_{i=1}^{f_0} \tau_i(z)\,\alpha_i$. Alors

$$\psi(\alpha) = \sum_{j=1}^{f_0} \alpha_j \sum_{i=0}^{f_0} \tau_i(z)\,\varphi_{ij}(z) = 0.$$

Donc, on a succésivement

$$\begin{aligned}
\varphi_{f_0,f_0}\,\tau_{f_0} &= 0,\\
\varphi_{f_0-1,f_0-1}\,\tau_{f_0-1} + \varphi_{f_0,f_0-1}\,\tau_{f_0} &= 0,\\
&\cdots\cdots\cdots\cdots\cdots\\
\varphi_{ii}\,\tau_i + \cdots\cdots + \varphi_{f_0,i}\,\tau_{f_0} &= 0,\\
&\cdots\cdots\cdots\cdots\cdots\\
\varphi_{11}\,\tau_1 + \cdots\cdots + \varphi_{f_0,1}\,\tau_{f_0} &= 0.
\end{aligned}$$

Ce qui entraîne, puisque, si $i \neq 1$, φ_{ii} est premier avec $z^f - \xi^{q_0}\frac{h}{\delta}$, que $\tau_i(z) = 0$ $(i = 2, 3, .., f_0)$ et que $\tau_1(z) \equiv 0 \pmod{\mathcal{P}_2}$.

Soit $\beta \oplus \gamma$ un élément quelconque de $\Omega(K)^{\left(\frac{E}{p^v(p-1)}\right)} \oplus \Omega(K)^{(q_0)}$. Soient

$$\beta = \sum_{i=1}^{f_0} \tau'_i(z)\,\alpha_i, \qquad \gamma = \sum_{i=1}^{f_0} \tau''_i(z)\,\alpha_i.$$

Il est évident qu'on peut trouver des polynomes $\lambda_2(z), \lambda_3(z), \ldots, \lambda_{f_0}(z)$ tels que

$$\beta - \gamma - \sum_{i=2}^{f_0} \lambda_i(z)\,\psi(\alpha_i) = \sum_{j=1}^{f_0} \alpha_j\left(\tau'_j(z) - \tau''_j(z) - \sum_{i=1}^{f_0} \lambda_i(z)\,\varphi_{ij}(z)\right)$$

prenne la forme $\lambda(z)\,\alpha_1$. De lors, posons

$$\varphi_2(z) = \tau'_2(z), \quad \varphi_3(z) = \tau'_3(z), \ldots, \varphi_{f_0}(z) = \tau'_{f_0}(z),$$

et définissons $\varphi_1(z)$ par deux congruences

$$\varphi_1(z) \equiv -\lambda(z) + \tau'_1(z) \pmod{\mathcal{P}_1}, \quad \varphi_1(z) \equiv \tau'_1(z) \pmod{\mathcal{P}_2},$$

ce qui est possible parce que $\mathcal{P}_1$ et $\mathcal{P}_2$ sont premiers entre eux. Alors,

$$\varphi_1(z)\,(\alpha_1 \oplus \alpha_1) + \varphi_2(z)\,(\alpha_2 \oplus \alpha_2) + \ldots + \varphi_{f_0}(z)\,(\alpha_{f_0} \oplus \alpha_{f_0}) = (\beta \oplus \gamma) +$$

$$+ ((\varphi_1(z) - \tau'_1(z))\,\alpha_1 \oplus)(\varphi_1(z) - \tau'_1(z) + \lambda(z))\,\alpha_1 + \lambda_2(z)\,\psi(\alpha_2) + \ldots + \lambda_{f_0}(z)\,\psi(\alpha_{f_0})) \equiv$$

$$\equiv \beta \oplus \gamma \pmod{\overline{P}_{\frac{E}{p^v(p-1)}} \oplus \overline{P}_{q_0}},$$

parce que

$$\varphi_1(z) - \tau'_1(z) \equiv 0 \pmod{\mathcal{P}_2} \text{ et } \varphi_1(z) - \tau'_1(z) + \lambda(z) \equiv 0 \pmod{\mathcal{P}_1}.$$

Donc $\{\alpha_1 \oplus \alpha_1,\ \alpha_2 \oplus \alpha_2, \ldots, \alpha_{f_0} \oplus \alpha_{f_0}\}$ est une base de

$$\Omega(K)^{\left(\frac{E}{p^v(p-1)}\right)} \oplus \Omega(K)^{(q_0)}/\overline{P}_{\frac{E}{p^v(p-1)}} \oplus \overline{P}_{q_0},$$

et $A(q_0)$-rang de $\mathfrak{U}/\overline{\mathfrak{U}}$ ne dépasse pas $(n_0 - f_0) + f_0 = n_0$, ce qui prouve la proposition. Il est impossible, $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n_0}\}$ étant une Γ-base de $\mathfrak{U}/\overline{\mathfrak{U}}$, que $\varepsilon_1\Gamma, \varepsilon_2\Gamma, \ldots \varepsilon_{n_0}\Gamma \cap \overline{\mathfrak{U}} \neq \{1\}$, parce que alors $\varepsilon_1\Gamma\,\varepsilon_2\Gamma \ldots \varepsilon_{n_0}\Gamma \cap \overline{\mathfrak{U}} = \overline{\mathfrak{U}}$, et $\varepsilon_1\Gamma\,\varepsilon_2\Gamma \ldots \varepsilon_{n_0}\Gamma = (\varepsilon_1\Gamma\,\varepsilon_2\Gamma \ldots \varepsilon_{n_0}\Gamma)^2 \supseteq \varepsilon_1\Gamma\,\varepsilon_2\Gamma \ldots \varepsilon_{n_0}\Gamma.\overline{\mathfrak{U}} = \mathfrak{U}$ aurait le rang $> N$ par rapport à $\mathfrak{U}$*.

Si, dans les théorèmes précédents, on pose k égal au corps p-adique rationnel (c'est-à-dire si l'on pose $n_0 = 1$), on obtient l'énoncé suivant, qui généralise d'une manière très stricte la théorie des racines primitives de Euler.

Théorème 17: *Si K est un surcorps galoisien, et sans ramifications supérieures, du corps p-adique rationnel, a) si K est régulier, il existe une 1-unité ε_0 de K telle que toute autre 1-unité ε de K peut se mettre sous la forme $\varepsilon = \varepsilon_0^{\zeta}$ $(\zeta \in \Gamma)$; $\varepsilon_0^{\zeta} = 1$ a lieu si, et seulement si $\zeta = 0$; b) si K est irrégulier, il existe deux 1-unités $\varepsilon_0, \varepsilon_1$ de K telles que toute autre 1-unité de K peut se mettre sous la forme $\varepsilon_0^{\zeta_0}\varepsilon_1^{\zeta_1}$ $(\zeta_0, \zeta_1 \in \Gamma)$; en particulier, si le dégré de K est premier à p, on peut prendre $\varepsilon_1 = \eta_1$, η_1 étant une racine primitive p-ième de l'unité, et alors $\eta_1^{\zeta}\varepsilon_0^{\zeta_0} = 1$ n'a lieu que si $\eta_1^{\zeta} = 1$, $\zeta_0 = 0$*

(Reçu le 16 avril 1938.)