

SÉMINAIRE DE MATHÉMATIQUES

ANDRÉ WEIL

Corps p -adiques

Séminaire de Mathématiques (Julia), tome 1 (1933-1934), exp. n° 8, p. 1-18

http://www.numdam.org/item?id=SMJ_1933-1934__1__A8_0

© École normale supérieure, Paris, 1933-1934, tous droits réservés.

L'accès aux archives du séminaire de mathématiques implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

I. - CORPS SEMINAIRE DE MATHÉMATIQUES

Soient K le corps des nombres rationnels, $K = \mathbb{Q}$ ($\mathbb{Q}$)
 un corps Première année 1933-1934, défini comme l'ensemble
 des fractions rationnelles à coefficients dans K , d'une racine
 d'une équation de degré n irréductible dans K . K peut
 être la Théorie des Groupes et des Algèbres sur K , de base
 $1, \theta, \theta^2, \dots, \theta^{n-1}$ ou plus généralement de base $\xi, \xi^2, \dots, \xi^{n-1}$
 si les ξ_i sont n éléments de K linéairement indépendants par
 rapport à K ; l'élément générique de K sera ainsi :

H. - CORPS p -ADIQUES

$$\xi = x_0 + x_1 \theta + x_2 \theta^2 + \dots + x_{n-1} \theta^{n-1}$$

Dans K on distingue les entiers, racines d'une équation
 normale (coefficient de $x^n = 1$) à coefficients entiers ra-
 tionnels. On démontre que ces entiers forment un anneau.

Un idéal dans K est un ensemble α d'éléments α tels que
 1°- si $\alpha \in \alpha$, $\beta \in \alpha$, $\alpha \pm \beta \in \alpha$ (α est module);
 2°- si $\alpha \in \alpha$ et si ω est entier, $\alpha \omega \in \alpha$;
 3°- il y a un entier m tel que $m \omega$ soit entier pour tout
 $\alpha \in \alpha$. Si tous les $\alpha \in \alpha$ sont entiers, l'idéal α est dit
 entier. A chaque élément ξ de K correspond l'idéal prin-
 cipal (ξ) formé de tous les éléments $\xi \omega$, ω entier.

On démontre que tout idéal α est une base $\alpha_1, \alpha_2, \dots, \alpha_n$
 telle que tout $\alpha \in \alpha$ soit de la forme $\alpha = m_1 \alpha_1 + \dots + m_n \alpha_n$
 m_i entiers rationnels, et réciproquement. En particulier,
 l'idéal (1) engendré des entiers de K est une telle base $\omega_1, \omega_2, \dots$

Corps p-adiques

Si M est un ensemble, on écrit des congruences entre entiers de K : $\omega \equiv \eta \pmod{M}$ signifie $\omega - \eta \in M$. Il n'y

I. - Corps de nombres algébriques : rappel de notions connues

Soient R le corps des nombres rationnels, $k = R(\theta)$ un corps algébrique fini de degré n , défini comme l'ensemble des fonctions rationnelles, à coefficients dans R , d'une racine θ d'une équation de degré n irréductible dans R . k peut être considéré comme système hypercomplexe sur R , de base $1, \theta, \theta^2, \dots, \theta^{n-1}$, ou plus généralement de base $\xi_1, \xi_2, \dots, \xi_n$ si les ξ_i sont n éléments de k linéairement indépendants par rapport à R ; l'élément générique de k sera ainsi :

$$\xi = x_1 \xi_1 + \dots + x_n \xi_n, \quad x_i \in R.$$

Dans k on distingue les entiers, racines d'une équation normée (coefficient de $x^n = 1$) à coefficients entiers rationnels. On démontre que ces entiers forment un anneau.

Un idéal dans k est un ensemble $\mathfrak{A}$ d'éléments α tels que :

- 1°- si $\alpha \in \mathfrak{A}$, $\beta \in \mathfrak{A}$, $\alpha \pm \beta \in \mathfrak{A}$ ($\mathfrak{A}$ est module) ;

- 2°- si $\alpha \in \mathfrak{A}$ et si ω est entier, $\alpha \omega \in \mathfrak{A}$;

- 3°- il y a un entier m tel que $m\alpha$ soit entier pour tout $\alpha \in \mathfrak{A}$. Si tous les $\alpha \in \mathfrak{A}$ sont entiers, l'idéal $\mathfrak{A}$ est dit entier. A chaque élément ξ de k correspond l'idéal principal (ξ) formé de tous les éléments $\xi \omega$, ω entier.

On démontre que tout idéal $\mathfrak{A}$ a une base $\alpha_1, \alpha_2, \dots, \alpha_n$ telle que tout $\alpha \in \mathfrak{A}$ soit de la forme $\alpha = m_1 \alpha_1 + \dots + m_n \alpha_n$, m_i entiers rationnels, et réciproquement. En particulier, l'idéal (1) anneau des entiers de k a une telle base $\omega_1, \omega_2, \dots, \omega_n$.

Si $\mathfrak{m}$ est idéal entier, on écrit des congruences entre entiers de k : $\omega \equiv \eta \pmod{\mathfrak{m}}$ signifie $\omega - \eta \in \mathfrak{m}$. Il n'y a dans k qu'un nombre fini d'entiers incongrus entre eux de mod. $\mathfrak{m}$.

Un idéal entier $\mathfrak{p}$ est dit premier si $\omega\eta \equiv 0 \pmod{\mathfrak{p}}$ entraîne que $\omega \equiv 0 \pmod{\mathfrak{p}}$ ou bien $\eta \equiv 0 \pmod{\mathfrak{p}}$. Cela posé, on démontre : Tout idéal (entier ou non) peut s'exprimer d'une manière et d'une seule (à l'ordre près) sous forme d'un produit de puissances (à exposants positifs ou négatifs) d'idéaux premiers.

2.- Considérons un idéal entier $\mathfrak{m}$ et les classes de restes mod. $\mathfrak{m}$, qu'on obtient en identifiant entre eux les entiers de k qui sont congrus mod. $\mathfrak{m}$: ces classes forment un anneau à un nombre fini d'éléments. Pour que cet anneau soit sans diviseurs de zéro, il faut et il suffit évidemment que $\mathfrak{m}$ soit un idéal premier $\mathfrak{p}$; dans ce cas, l'anneau est un corps (car ses éléments $\neq 0$ forment par rapport à la multiplication un groupe fini) ; c'est un corps fini ou champ de Galois : on peut le considérer comme extension finie du corps des entiers rationnels mod. p , p étant le plus petit entier rationnel contenu dans $\mathfrak{p}$ (p est premier, car les éléments rationnels de $\mathfrak{p}$ forment un idéal premier de l'anneau des entiers rationnels).

Au contraire, l'anneau des classes de restes mod. $\mathfrak{p}^n$ n'est plus un corps : c'est pour tourner la difficulté ré-

sultent de l'apparition de tels anneaux que Hensel a introduit les nombres p -adiques ; on y est conduit en considérant simultanément les classes de restes mod. p^n quelque soit n .

3.- Nombres p -adiques : 1ère définition

Soit p premier rationnel. On considère une suite d'éléments $a_1, a_2, \dots, a_n, \dots$, a_n représentent une classe de restes mod. p ; de telle sorte que l'on ait $a_{n+k} \equiv a_n \pmod{p^n}$ quels que soient n, k . Une telle suite sera appelée un entier p -adique A . A tout entier rationnel a correspond évidemment une telle suite, celle qu'on obtient en prenant $a_n = a \pmod{p^n}$; la réciproque n'est pas vraie ; cette suite s'appellera l'entier p -adique a . Les entiers p -adiques forment un anneau : si

$$A = (a_1, a_2, \dots) \quad \text{et} \quad B = (b_1, b_2, \dots)$$

$$\text{on écrira : } A + B = (a_1 + b_1, a_2 + b_2, \dots)$$

$$\text{et } A.B = (a_1.b_1, \dots)$$

Si $a_n \equiv 0 \pmod{p^n}$ d'où $a_{n+k} \equiv 0 \pmod{p^n}$ on écrira $A \equiv 0 \pmod{p^n}$

Si $A \equiv 0 \pmod{p^n}$ quel que soit n , $A = 0$: il en résulte que

l'anneau des A est sans diviseur de zéro, car si $A \not\equiv 0 \pmod{p^n}$

$B \not\equiv 0 \pmod{p^n}$, on a $A.B \not\equiv 0 \pmod{p^{m+n}}$. On peut donc former

au moyen des A , un corps des quotients ; -le corps des nombres

p -adiques - comme on forme le corps des rationnels au moyen

des entiers ordinaires. Il est clair que si $B \not\equiv 0 \pmod{p}$,

A/B est encore entier p -adique ; en particulier une fraction

rationnelle a/b est entier p -adique si b est premier à p .
 D'ailleurs si $B \equiv 0 \pmod{p^n}$ et $\not\equiv 0 \pmod{p^{n+1}}$, $B = p^n \cdot B_1$
 et $B_1 \not\equiv 0 \pmod{p}$, donc tout nombre p -adique A/B peut s'écrire
 $\frac{C}{p^n}$ $C = A/B_1$ étant un entier p -adique.

4.- Rien n'empêche de procéder de même pour un corps k et un idéal premier $\mathfrak{p}$. Mais nous reprendrons la question par une autre méthode, qui est fournie par la notion de valuation.

Par valuation dans K , on entend une fonction $\varphi(\xi) \geq 0$ non constante, des éléments de k , telle que

$$\varphi(\xi \eta) = \varphi(\xi) \cdot \varphi(\eta) \quad (A)$$

$$\varphi(\xi + \eta) \leq \varphi(\xi) + \varphi(\eta) \quad (B)$$

(On entend aussitôt $\varphi(0) = 0$, $\varphi(\pm 1) = 1$).

(B) signifie que le corps k devient un espace métrique si l'on prend $\varphi(\xi - \xi')$ comme distance des éléments ξ, ξ' .
 On en déduit une notion de convergence : une suite ξ_n converge si $\varphi(\xi_m - \xi_n) < \varepsilon$ pour m, n assez grands ; s'il existe alors ξ tel que $\lim. \varphi(\xi - \xi_n) = 0$, ξ sera dit limite de la suite. En analyse on définit les nombres irrationnels à partir des nombres rationnels comme limites de suites convergentes (définition de Cantor), la distance étant la valeur absolue de la différence. On obtient ainsi un corps parfait (au sens topologique), le corps des nombres réels où le corps des rationnels est plongé et est partout dense. De même ici : toute suite convergente ξ_n qui n'a pas pour

limite un ξ dans k aura par définition une limite Ξ ;
 par définition $\varphi(\Xi)$ sera $\lim. \varphi(\xi_n)$ (qui existe car

$$|\varphi(\xi_m) - \varphi(\xi_n)| \leq \varphi(\xi_m - \xi_n) \text{ d'après (B)).}$$

$\xi \pm \eta$ et $\xi\eta$ sont, d'après (B) et (A), fonctions conti-
 nues de ξ, η , au sens de la distance φ ; de même $\frac{1}{\xi}$ pour
 $\xi \neq 0$; donc si $\Xi = \lim. \xi_n$, $H = \lim. \eta_n$, on peut défi-
 nir $\Xi \pm H$ et $\Xi \cdot H$ comme limites de $\xi_n \pm \eta_n$ et $\xi_n \cdot \eta_n$
 respectivement. De même, $\frac{1}{\Xi} = \lim. \frac{1}{\xi_n}$ si $\Xi \neq 0$.

$\Xi = \Xi'$ si $\Xi - \Xi' = 0$, c'est à dire si $\lim. (\xi_n - \xi'_n) = 0$.

Les nouveaux nombres Ξ forment avec les anciens un corps,
 qui sera d'ailleurs espace métrique pour la distance φ et k
 y est partout dense ; ce corps est dit la fermeture de k par
 φ .

5.- Mais il faut distinguer deux cas : Soit d'abord (valua-
 tion de l'ère espèce), $\varphi(a) \leq 1$ pour au moins un entier
 naturel $a > 1$. Soit m un entier naturel, écrivons-le dans
 le système de base a ; si $m < a^k$ on aura

$$m = c_0 + c_1 a + \dots + c_{k-1} a^{k-1}, \quad 0 \leq c_i < a$$

Soit φ_0 le plus grand des nombres $\varphi(1), \varphi(2), \dots, \varphi(a-1)$
 on aura par (B) :

$$\begin{aligned} \varphi(m) &\leq \varphi(c_0) + \varphi(c_1) \varphi(a) + \dots + \varphi(c_{k-1}) \varphi(a^{k-1}) \\ &\leq \varphi_0 [1 + \varphi(a) + \varphi(a)^2 + \dots + \varphi(a)^{k-1}] \end{aligned}$$

donc $\varphi(m) \leq k \varphi_0$, et de même $\varphi(m^\nu) \leq k^\nu \varphi_0$.

quel que soit ν , donc $\varphi(m) \leq 1$

Soient alors ξ, η dans k , et par exemple $\varphi(\xi) \leq \varphi(\eta)$
 on a : $\varphi[(\xi + \eta)^\nu] = [\varphi(\xi + \eta)]^\nu$

$$\leq \varphi(\xi^v) + \varphi(c_1^v) \varphi(\xi^{v-1}) \varphi(\eta) + \varphi(c_2^v) \varphi(\xi^{v-2}) \varphi(\eta^2) + \dots$$

$$\leq (v+1) \varphi(\xi)^v$$

quel que soit v , d'où : $\varphi(\xi + \eta) \leq \varphi(\eta)$ $\varphi(c)$.

Soit maintenant ω entier : $\omega = m, w_1 + \dots + m_n w_n$

donc par (C) $\varphi(\omega)$ est $\leq$ au plus grand des nombres $\varphi(w_1)$

$\dots \varphi(w_n)$, donc borné, donc ≤ 1 , car sinon $\varphi(w^v)$

serait non borné. Considérons les ω tels que $\varphi(\omega) < 1$;

il en existe, sinon φ serait constante. Ils forment un idéal

si d'après (C), et un idéal premier, d'après (A); soit $\mathfrak{f}$ cet

idéal, π un entier $\equiv 0(\mathfrak{f})$ et $\not\equiv 0(\mathfrak{f}^2)$, et soit

$\varphi(\pi) = w < 1$. Soit ξ un nombre quelconque de k :

si l'expression de (ξ) comme produit de puissances d'idéaux

premiers contient un facteur $\mathfrak{f}^m$, avec $m \geq 0$, ce facteur

est dit la contribution de $\mathfrak{f}$ à ξ ; sinon, on prend $m = 0$

et la contribution de $\mathfrak{f}$ à ξ sera 1; soit donc en tout cas,

$\mathfrak{f}^m$ cette contribution, l'expression de $\xi \pi^{-m}$ ne contient plus

$\mathfrak{f}$ donc $\xi \pi^{-m}$ est quotient de deux entiers $\not\equiv 0(\mathfrak{f})$, et l'on

a : $\varphi(\xi \pi^{-m}) = 1$, d'où $\varphi(\xi) = w^m$. φ est ainsi

complètement définie. Réciproquement, à tout idéal premier

$\mathfrak{f}$ et à tout $w < 1$ correspond une valuation φ . La fer-

meture de k par cette valuation est dite le corps $\mathfrak{f}$ -adique

déduit de k : il ne dépend visiblement pas de w . On convient

de prendre w de manière que si p est le nombre premier (ra-

tional) multiple de $\mathfrak{f}$, l'on ait $\varphi(p) = -$: φ est alors

la valeur absolue $\mathfrak{f}$ -adique dans k .

6.- Si $\varphi > 1$ pour tous les entiers rationnels > 1 , écrivons, comme plus haut, l'entier naturel m dans le système de base a , on aura :

$$\varphi(m) \leq \varphi_0 [1 + \varphi(a) + \dots + \varphi(a)^{k-1}] = \varphi_0 \frac{\varphi(a)^k - 1}{\varphi(a) - 1} \varphi(a)^{k-1}$$

$$\varphi(m) \leq \varphi(a)^k$$

De même, quels que soient les entiers h, k , tels que $m^h < a^k$, on a $\varphi(m) \leq \varphi(a)^k$; $\frac{h}{k} < \frac{\log a}{\log m}$ entraîne

$$\frac{\log \varphi(a)}{\log \varphi(m)} \geq \frac{h}{k} \quad \text{donc} \quad \frac{\log \varphi(a)}{\log \varphi(m)} \geq \frac{\log a}{\log m}$$

et de même $\frac{\log \varphi(m)}{\log \varphi(a)} \geq \frac{\log m}{\log a}$ et par suite :

$$\varphi(a) = |a|^\lambda \quad \lambda = \text{cte.} \quad \text{D'ailleurs, par (B),}$$

$$\varphi(2) \leq \varphi(1) + \varphi(1) = 2, \text{ donc } \lambda \leq 1. \text{ Réciproquement,}$$

$\varphi(x) = |x|^\lambda$ fournit, quel que soit $\lambda \leq 1$, une valuation du corps R , sa fermeture $\mathcal{N}$ étant le corps des nombres réels. Si k est quelconque, il contient en tout cas R , et sa fermeture contient $\mathcal{N}$ (plus exactement, un corps isomorphe à $\mathcal{N}$). Si k y est contenu, c'est donc qu'il existe

un corps de nombres algébriques réels k_1 , isomorphe à k et tel que si, à ξ dans k correspond ξ_1 dans k_1 ,

$$\varphi(\xi) = |\xi|^\lambda : \text{à tout corps } k_1 \text{ et à tout } \lambda \leq 1 \text{ cor-}$$

respond une valuation de k . Si k n'est pas dans $\mathcal{N}$, formons dans la fermeture de k_1 le plus petit corps k_2 qui contienne à la fois k et $\mathcal{N}$: c'est une extension finie de $\mathcal{N}$ donc isomorphe au corps des nombres complexes ; soit, dans

ce corps, $\varphi(\xi_n) \leq 1$, donc $\xi_n = \frac{\omega_n}{\eta_n}$, ω_n et η_n étant

ce corps, l'élément $z = e^{i\theta}$; $\varphi(z^\nu) = \varphi(\cos \nu\theta + i \sin \nu\theta)$
 $\leq |\cos \nu\theta|^\lambda + \varphi(1) \cdot |\sin \nu\theta|^\lambda$ sera borné quel que soit
 $\nu \geq 0$, donc $\varphi(e^{i\theta}) = 1$; et par suite, z étant un nom-
bre complexe quelconque, $\varphi(z) = \varphi(|z|) = |z|^\lambda$. Il y a donc
dans ce cas, un corps de nombres algébriques complexes k_1 ,
isomorphe à k , et si à ξ dans k correspond ξ_1 dans k_1 , on
a $\varphi(\xi) = |\xi_1|^\lambda$. Réciproquement, à un tel corps k_1 , et
à $\lambda \leq 1$, correspond une valuation dans k .

D'ailleurs, si k est de degré n , il y a n manières de
représenter k (supposé donné comme corps abstrait) au moyen
d'un corps de nombres algébriques réels ou complexes k_1 .
Il semblerait donc qu'il y ait n familles de valuations de k ,
mais en réalité deux corps k_1 , imaginaires conjugués, don-
nent évidemment les mêmes valuations. Dans tout autre cas
deux corps k_1 donnent des valuations distinctes.

Chaque famille de valuations ainsi obtenue est dite
(par définition) correspondre à un idéal premier à l'infini
de k .

7.- Revenons aux corps η -adiques. L'analyse dans ces corps
repose sur le fait suivant, conséquence immédiate de (C) :
Pour que la série $\sum_{n=1}^{\infty} \xi_n$ converge, il faut et il suffit
que ξ_n tende vers 0.

Parmi les ξ_n , on distingue les entiers η -adiques Ω ,
limites d'entiers de k . Pour un tel nombre, on a $\varphi(\Omega) \leq 1$.
Réciproquement, soit $\Omega = \lim. \xi_n$ et $\varphi(\Omega) \leq 1$: pour n
assez grand, $\varphi(\xi_n) \leq 1$, donc $\xi_n = \frac{\omega_n}{\eta_n}$, ω_n et η_n étant

entiers et $\eta_n \not\equiv 0 \pmod{\mathfrak{y}}$; on pourra alors trouver ω'_n entier tel que $\omega_n = \eta_n \omega'_n \pmod{\mathfrak{y}^n}$ et Ω sera limite des ω'_n .

Les entiers $\mathfrak{y}$ -adiques forment un anneau. A tout Ω entier correspond, quel que soit n , une classe de restes mod. $\mathfrak{y}^n$ qui est celle à laquelle appartiennent tous les entiers de K suffisamment voisins de Ω (au sens de la distance φ) : Ω est d'ailleurs bien défini par cette suite de classes de restes (cf. par. 3). L'inverse d'un entier $E \not\equiv 0 \pmod{\mathfrak{y}}$ est encore entier : car si $E \equiv \lim. \omega_n$, $\omega_n \not\equiv 0 \pmod{\mathfrak{y}}$, et on aura $1/E = \lim. \eta_n$, les entiers η_n étant tels que $\omega_n \eta_n \equiv 1 \pmod{\mathfrak{y}^n}$. Ces entiers s'appellent unités $\mathfrak{y}$ -adiques ; ce sont les nombres pour lesquels $\varphi(E) = 1$. Si $\varphi(\pi) = \mathfrak{y}^m$, on aura $\pi = \pi^m E$, E étant une unité.

Les entiers $\not\equiv 0 \pmod{\mathfrak{y}}$ forment, dans l'anneau des entiers $\mathfrak{y}$ -adiques, un idéal premier, qui s'appellera encore l'idéal $\mathfrak{y}$. Tout idéal dans l'anneau est puissance de $\mathfrak{y}$: soit en effet, dans un tel idéal, $\Omega = \pi^m E$ un nombre où l'exposant m de π soit le plus petit possible ; l'idéal contiendra π^m , donc tous les nombres d'exposant $\geq m$, et, par hypothèse, ceux-là seulement : il se confond avec $\mathfrak{y}^m$. De plus tout idéal est idéal principal : car $\mathfrak{y}^m = (\pi^m) = (\pi^m E)$, E étant une unité quelconque.

Prenons des entiers $\mathfrak{y}$ -adiques formant un système complet de restes mod. $\mathfrak{y}$: nous pouvons par exemple choisir pour cela des entiers de K , $\xi_1, \xi_2, \dots, \xi_q$ (d'ailleurs $q =$ norme de $\mathfrak{y} = p^F$, F étant le degré de $\mathfrak{y}$). Soit π

un entier quelconque, il sera congru mod. φ à l'un des ξ , soit ξ_{i_0} ; $\frac{\Xi - \xi_{i_0}}{\pi}$ sera alors entier, et $\equiv \xi_{i_1} (\varphi)$. Soit donc en général: $\Xi_n = \frac{\Xi_{n-1} - \xi_{i_{n-1}}}{\pi} \equiv \xi_{i_n} (\varphi)$; Ξ pourra s'exprimer par un développement en série convergente suivant les puissances de π :

$$\Xi = \xi_{i_0} + \xi_{i_1} \pi + \dots + \xi_{i_n} \pi^n + \dots$$

et l'on obtiendra tous les entiers φ -adiques une fois et une seule en donnant aux coefficients les q valeurs incongrues mod. φ (Donc la puissance de leur ensemble est celle du continu). Si Ξ n'est pas entier, $\pi^m \Xi$ sera entier pour m assez grand, et Ξ pourra encore s'exprimer par un développement suivant les puissances croissantes de π :

$$\Xi = \sum_{v=0}^{\infty} \xi_{i_v} \pi^{-m+v}$$

Enfin, on a un principe de Bolzano: Si une suite de nombres Ξ_n est "bornée", on peut en extraire une suite convergente. L'hypothèse signifie que $\varphi(\Xi_n) < M$, donc qu'il y a m tel que tous les $\pi^m \Xi_n$ soient entiers; dans cette suite d'entiers, il y en a sûrement une infinité qui ont même reste mod. φ : ils forment une suite partielle, d'où l'on peut à nouveau extraire une suite d'entiers qui ont même reste mod. φ^2 et ainsi de suite. La suite diagonale est alors convergente.

8.- Théorie des extensions finies. Soient k_{φ} le corps φ -adique déduit de k et de l'idéal premier φ dans k , p étant le nombre premier $\equiv 0 (\varphi)$, les limites de nombres

rationnels forment dans $k_{\mathfrak{p}}$ un sous-corps $R_{\mathfrak{p}}$, qui n'est autre que le corps des nombres p -adiques. $k_{\mathfrak{p}}$ est extension algébrique finie de $R_{\mathfrak{p}}$: soit en effet, $\overline{\omega}$ un nombre de $k_{\mathfrak{p}}$; pour m assez grand, $p^m \overline{\omega} = \Omega$ sera un entier, limite d'une suite d'entiers $\omega = m_1 \omega_1 + m_2 \omega_2 + \dots + m_n \omega_n$ de k , les m_i étant des entiers rationnels. D'après le principe de Bolzano, on peut extraire de cette suite une autre où chacun des m_i converge vers un entier p -adique M_i , d'où

$$\Omega = M_1 \omega_1 + \dots + M_n \omega_n$$

et $\overline{\omega} = X_1 \omega_1 + X_2 \omega_2 + \dots + X_n \omega_n$ les X_i étant des nombres de $R_{\mathfrak{p}}$: $k_{\mathfrak{p}}$ est donc un $R_{\mathfrak{p}}$ -module fini, donc, comme on sait, une extension algébrique finie, de degré $\leq n$. Avec les notations des systèmes hypercomplexes, on peut écrire $k_{\mathfrak{p}} = k \times R_{\mathfrak{p}}$.

Plus généralement, si k' est un sous-corps de k , et $\mathfrak{p}'$ l'idéal premier de k' , qui est multiple de $\mathfrak{p}$, les limites de nombres de k' forment dans $k_{\mathfrak{p}}$ le corps $k'_{\mathfrak{p}}$, intermédiaire entre $R_{\mathfrak{p}}$ et $k_{\mathfrak{p}}$ et $k_{\mathfrak{p}}$ en est donc extension finie. Réciproquement, nous allons voir que toute extension finie de corps $\mathfrak{p}$ -adiques peut s'obtenir de cette manière.

La théorie de ces extensions finies se fonde sur le lemme suivant :

Un polynôme irréductible dans le corps $\mathfrak{p}$ -adique $k_{\mathfrak{p}}$ est irréductible ou puissance de polynôme irréductible modulo $\mathfrak{p}$.

Soit H un élément de R : H et ses conjugués $H^1, H^2, \dots, H^{(n-1)}$ seront les racines d'une équation normale (coefficients

Soit en effet $F(x)$ un polynôme de degré n à coefficient $\mathcal{U}$ -adiques ; montrons que si $F(x) \equiv f(x).g(x) \pmod{\mathcal{U}}$, f et g étant deux polynômes premiers entre eux mod. $\mathcal{U}$, F ne peut être irréductible. Soient r, s , les degrés de f et g (avec $r+s = n$) On pourra déterminer par récurrence des polynômes f_n et g_n de degrés r, s , de sorte que l'on ait :

$$F(x) = (f + \pi f_1 + \pi^2 f_2 + \dots + \pi^n f_n + \dots)(g + \pi g_1 + \dots + \pi^n g_n + \dots)$$

car si on pose

$$\varphi_{n-1} = f + \pi f_1 + \dots + \pi^{n-1} f_{n-1}, \quad \psi_{n-1} = g + \pi g_1 + \dots + \pi^{n-1} g_{n-1},$$

et que l'on suppose que $F(x) \equiv \varphi_{n-1}(x) \cdot \psi_{n-1}(x) \pmod{\mathcal{U}^n}$, il suffira de déterminer f_n, g_n , par la condition :

$$\pi^n (\varphi_{n-1} g_n + \psi_{n-1} f_n) \equiv F - \varphi_{n-1} \psi_{n-1} \pmod{\mathcal{U}^{n+1}}$$

c'est à dire :

$$f g_n + g f_n = \frac{F - \varphi_{n-1} \psi_{n-1}}{\pi^n} \pmod{\mathcal{U}}$$

ce qui est possible, le second membre étant entier et f, g premiers entre eux. $F(x)$ apparaît ainsi comme produit de deux séries (évidemment convergentes) qui représentent deux polynômes $\mathcal{U}$ -adiques de degrés r, s , d'ailleurs premiers entre eux.

9.- Soit alors $k_{\mathcal{U}}$ un corps $\mathcal{U}$ -adique, φ la valeur absolue dans ce corps, et soit $\mathcal{K} = k_{\mathcal{U}}(\theta)$ une extension finie de degré n , engendrée par une racine θ d'une équation de degré n irréductible dans $k_{\mathcal{U}}$, dont les autres racines seront $\theta', \theta'', \dots, \theta^{(n-1)}$.

Soit H un élément de $\mathcal{K}$: H et ses conjugués $H', H'', \dots, H^{(n-1)}$ seront les racines d'une équation normée (coefficient

de $x^n = 1$) bien déterminée à coefficients dans $K_{\mathfrak{f}}$; et sera dit entier si ces coefficients sont des entiers de $K_{\mathfrak{f}}$. Soit nH la norme de H , c'est à dire $(-1)^n \times$ le terme constant de cette équation. Posons $\varphi(H) = [\varphi(nH)]^{\frac{1}{n}}$: si H est dans $K_{\mathfrak{f}}$, cette fonction coïncide bien avec la valeur absolue. Evidemment $\varphi(H \cdot H_1) = \varphi(H) \cdot \varphi(H_1)$. Démontrons les deux théorèmes suivants :

1.- Pour que H soit entier, il faut et il suffit que $\varphi(H) \leq 1$, c'est à dire que nH soit entier.

2.- Si $\varphi(H) \leq \varphi(H_1)$, $\varphi(H + H_1) \leq \varphi(H_1)$

1.- En effet, la condition est évidemment nécessaire. Soit donc nH entier, et soit π^k le plus petit dénominateur commun de l'équation normée $F(x) = 0$ à laquelle satisfont H et ses conjugués. Si $k > 0$, $\pi^k F(x)$ serait $\equiv x^r g(x) \pmod{\mathfrak{f}}$ x^r et $g(x)$ étant premiers entre eux mod. $\mathfrak{f}$ (et $r > 0$). $F(x)$ serait donc, d'après la démonstration du lemme, produit de deux polynômes premiers entre eux, ce qui est impossible ; par suite, $k = 0$ et H est entier.

2.- On aura $\varphi\left(\frac{H}{H_1}\right) \leq 1$, donc $\frac{H}{H_1}$ est entier, donc $1 + \frac{H}{H_1}$ l'est aussi, et $\varphi\left(1 + \frac{H}{H_1}\right) \leq 1$.

On peut alors étendre au corps $\bar{K}$ toute la théorie exposée aux prg. 5 et 7 pour les corps $\mathfrak{f}$ -adiques. Remarquons en effet que, si l'on pose $W = \varphi(\pi)$, $\log \varphi(H)$ est toujours un multiple entier de $\frac{1}{n} \log \frac{1}{W}$; et appelons $\log \frac{1}{W}$ la plus petite valeur de $|\log \varphi(H)|$; soit Π un

élément de $\mathcal{K}$ tel que $\varphi(\pi) = W$, l'idéal principal $(\pi) = \mathfrak{p}$ sera l'unique idéal premier de l'anneau des entiers de $\mathcal{K}$, et tous les idéaux de cet anneau seront des puissances de $\mathfrak{p}$; en particulier, pour l'idéal (π) de cet anneau que nous appellerons encore $\mathfrak{y}$, on aura $\mathfrak{y} = \mathfrak{p}^e$. Enfin, l'anneau des entiers de $\mathcal{K}$ est un module fini, de rang n , par rapport à l'anneau des entiers de $\mathcal{K}_{\mathfrak{y}}$: on le démontre en déterminant une base $H_1, H_2, \dots, H_n$ exactement comme lorsqu'il s'agit de l'anneau des entiers d'un corps de nombres algébriques fini par rapport à l'anneau des entiers rationnels; donc l'anneau des classes de restes mod. $\mathfrak{p}$ dans $\mathcal{K}$ est un module de rang fini $f \leq n$ par rapport au corps des classes de restes mod. $\mathfrak{y}$ dans $\mathcal{K}_{\mathfrak{y}}$, il a donc un nombre fini d'éléments, et comme il est sans diviseurs de zéro, c'est un corps fini (champ de Galois). De là on déduit, pour tous les résultats analogues à ceux du prg.7 ainsi que le lemme du prg.8.

10.- De plus, si q désigne, comme plus haut, le nombre des classes de restes mod. $\mathfrak{y}$ dans $\mathcal{K}_{\mathfrak{y}}$, q^f sera le nombre de classes de restes mod. $\mathfrak{p}$ dans $\mathcal{K}$; le nombre de classes de restes mod. $\mathfrak{p}^e = \mathfrak{y}$ dans $\mathcal{K}$ sera alors $(q^f)^e$, comme on le voit par exemple au moyen du développement suivant les puissances de π . Mais d'autre part, $H_1, H_2, \dots, H_n$ formant une base des entiers de $\mathcal{K}$ par rapport à l'anneau des entiers de $\mathcal{K}_{\mathfrak{y}}$, tout entier H de $\mathcal{K}$ est de la forme

$\sum_{i=1}^n \xi_i H_i$, les ξ_i étant des entiers de $k_{\mathfrak{p}}$: on obtient toutes les classes de restes mod. $\mathfrak{p}$ dans $k_{\mathfrak{p}}$ en donnant à chacun des ξ_i , q valeurs incongrues mod. $\mathfrak{p}$, et on obtient chacune une fois et une seule, car si $\sum \xi_i H_i = \sum \xi'_i H_i \pmod{\mathfrak{p}}$, $\sum \frac{\xi_i - \xi'_i}{\pi} H_i$ est entier, donc $\xi_i \equiv \xi'_i \pmod{\mathfrak{p}}$. Il y a donc dans $k_{\mathfrak{p}}$, q^n classes de restes mod. $\mathfrak{p}$: et par suite $n = e \cdot f$; f s'appelle le degré relatif de $\mathfrak{p}$ par rapport à $k_{\mathfrak{p}}$, e l'ordre de ramification de $\mathfrak{p}$ dans $k_{\mathfrak{p}}$.

f n'est autre chose que le degré du corps $k_{\mathfrak{p}}^*$ des classes de restes mod. $\mathfrak{p}$ dans $k_{\mathfrak{p}}$ par rapport au corps k^* des classes de restes mod. $\mathfrak{p}$ dans k ; dont il est extension algébrique finie. Soit η^* un élément générateur de $k_{\mathfrak{p}}^*$ par rapport à k^* , de sorte que $k_{\mathfrak{p}}^* = k^*(\eta^*)$; soit $F(X) = 0$ l'équation irréductible de degré f dont η^* est racine : les coefficients de F étant des classes de restes mod. $\mathfrak{p}$ dans $k_{\mathfrak{p}}$, on peut écrire $F = \xi_0 X^f + \xi_1 X^{f-1} + \dots + \xi_f \pmod{\mathfrak{p}}$ les ξ_i étant par exemple des entiers de k ; ce polynôme, étant irréductible dans k^* , l'est a fortiori dans $k_{\mathfrak{p}}$. Mais dans $k_{\mathfrak{p}}^*$, $F(X)$ possède une racine simple η^* ; d'après le lemme du prg. 8 il possède donc aussi une racine simple η dans $k_{\mathfrak{p}}$. Le corps $\bar{k} = k(\eta)$, extension algébrique de degré f de k , est donc contenu dans $k_{\mathfrak{p}}$; la valeur absolue $\mathfrak{p}$ y définit une valuation $\mathfrak{p}$ -adique, $\mathfrak{p}$ étant un idéal premier de $\bar{k}$; l'ensemble des limites d'éléments de $\bar{k}$ dans $k_{\mathfrak{p}}$ forme un corps $\bar{k}_{\mathfrak{p}} = k_{\mathfrak{p}}(\eta)$, extension de degré f de $k_{\mathfrak{p}}$; $k_{\mathfrak{p}}$ est extension algébrique de degré $\frac{n}{f} = e$ de $\bar{k}_{\mathfrak{p}}$. Mais

le corps des classes de restes mod. $\bar{y}$ dans $\bar{K}_{\bar{y}}$ est contenu dans $\mathcal{R}^*$, contient κ^* , et contient une racine η^* de $F(X) = 0$ il est donc de degré f par rapport à k^* , et se confond avec $\mathcal{R}^*$. Par suite le degré relatif de l'idéal $\mathfrak{p}$ par rapport à $\bar{K}$ est 1 ; celui de $\bar{y}$ par rapport à k est f , et puisque f est aussi le degré $\bar{n}$ de $\bar{K}_{\bar{y}}$ par rapport à $k_{\bar{y}}$, l'ordre de ramification $\bar{e} = \frac{\bar{n}}{f}$ de $\bar{y}$ dans $\bar{K}_{\bar{y}}$ est 1, on peut donc écrire $\bar{y} = \dots$.

Le corps $\bar{K}_{\bar{y}}$ s'appelle corps d'inertie de $\mathcal{R}$ par rapport à $k_{\bar{y}}$. Tout entier de $\mathcal{R}$ est congru mod. $\mathfrak{p}$ à un entier de $\bar{K}_{\bar{y}}$ et $\bar{K}_{\bar{y}}$ est le plus petit corps intermédiaire entre $k_{\bar{y}}$ et $\mathcal{R}$ qui possède cette propriété : c'est ce qui résulte du fait que $\bar{K}_{\bar{y}}$ est contenu, de même que dans $\mathcal{R}$, dans toute extension finie $\mathcal{R}_1$ de $k_{\bar{y}}$ dont l'idéal premier est de degré f par rapport à k .

11.- Pour achever de démontrer que $\mathcal{R}$ peut être considéré comme corps y -adique, prenons $\bar{K}$ comme point de départ, et, pour simplifier les notations, appelons-le désormais k . Cela revient à supposer que $f = 1$ et $e = n$. Soit $\mathcal{R} = k_y(\vartheta)$ ϑ étant supposé entier et racine d'une équation irréductible $\phi(X) = 0$ de degré n . On pourra prendre μ assez grand pour qu'il ne soit pas possible de trouver deux polynômes φ, ψ , à coefficients entiers dans k_y , tels que $\phi_0(X) \equiv \varphi(X) \cdot \psi(X) \pmod{y^\mu}$: sinon en effet on pourrait trouver une suite de valeurs de μ indéfiniment croissantes tels que les polynômes φ, ψ correspondants convergent, et

ϕ_0 ne serait pas irréductible. Dans ces conditions, tout polynôme $\phi(X)$ congru à $\phi_0 \bmod. \mathfrak{p}^r$ sera irréductible dans $k_{\mathfrak{p}}$: car sinon (en vertu d'un raisonnement bien connu) il serait produit de deux polynômes φ, ψ à coefficients entiers.

Supposons alors que $\phi'_0(\theta) \equiv 0 \pmod{\mathfrak{p}^{r-1}}$ et $\not\equiv 0 \pmod{\mathfrak{p}^r}$. On peut toujours écrire $\theta = \xi_0 + \xi_1 \pi + \dots + \xi_{r-1} \pi^{r-1} + \theta' \pi^r$ les ξ_i étant des entiers pris par exemple dans k , et θ' étant entier. Prenons un polynôme $\phi(X)$ à coefficients dans k et $\equiv \phi_0(X) \pmod{\mathfrak{p}^\alpha}$, α étant $\geq 2r$ et $\geq r$.

Nous allons montrer que l'on peut déterminer par récurrence

$\xi_r, \xi_{r+1}, \dots$ de façon que :

$$\theta = \xi_0 + \xi_1 \pi + \dots + \xi_{r-1} \pi^{r-1} + \xi_r \pi^r + \xi_{r+1} \pi^{r+1} + \dots$$

soit racine de $\phi(X) = 0$. Posons pour cela,

$$X_v = \xi_0 + \xi_1 \pi + \dots + \xi_v \pi^v$$

On a : $\theta = X_{r-1} + \theta' \pi^r$, donc :

$$0 = \phi(\theta) \equiv \phi_0(X_{r-1}) + \phi'_0(X_{r-1}) \cdot \theta' \pi^r \pmod{\mathfrak{p}^{2r}}$$

d'ailleurs $\phi'_0(X_{r-1}) \equiv \phi'_0(\theta) \pmod{\mathfrak{p}^r}$, donc

$$\phi'_0(X_{r-1}) \equiv 0 \pmod{\mathfrak{p}^{r-1}} \text{ et :}$$

$$\phi_0(X_{r-1}) \equiv 0 \pmod{\mathfrak{p}^{2r-1}} ;$$

par suite aussi $\phi(X_{r-1}) \equiv 0 \pmod{\mathfrak{p}^{2r-1}}$ puisque $\phi = \phi_0 \pmod{\mathfrak{p}^{2r}}$

De plus $\phi'(X_{r-1}) \equiv \phi'_0(X_{r-1}) \pmod{\mathfrak{p}^r}$, donc $\phi'(X_{r-1})$ est $\equiv 0 \pmod{\mathfrak{p}^{r-1}}$ et $\not\equiv 0 \pmod{\mathfrak{p}^r}$;

Supposons donc que l'on ait déterminé $\xi_r, \xi_{r+1}, \dots, \xi_{v-1}$ ($v \geq r$) de telle sorte que $\phi(X_{v-1}) \equiv 0 \pmod{\mathfrak{p}^{v+r-1}}$ et que $\phi'(X_{v-1})$ soit $\equiv 0 \pmod{\mathfrak{p}^{r-1}}$ et $\not\equiv 0 \pmod{\mathfrak{p}^r}$: nous ve-

Exemplaire n° 4

Institut Henri Poincaré
On peut quitter la Salle de Travail

nous de voir qu'il en est bien ainsi pour $v = r$.

Soit $X_v = X_{v-1} + \xi_v \pi^v$ on aura :

$$\phi(X_v) \equiv \phi(X_{v-1}) + \phi'(X_{v-1}) \xi_v \pi^v \quad (\pi^{2v})$$

donc on pourra déterminer ξ_v par la condition :

$$\xi_v \equiv - \frac{\phi(X_{v-1})}{\phi'(X_{v-1}) \pi^v} \quad (\pi)$$

le second membre est entier, on peut prendre pour ξ_v par exemple un entier de k . On aura bien $\phi(X_v) \equiv 0 \quad (\pi^{v+z})$, et

$\phi'(X_v)$ sera $\equiv 0 \quad (\pi^{v-1})$ et $\not\equiv 0 \quad (\pi^v)$. En poursuivant ainsi

on déterminera θ comme somme d'une série convergente ;

et $\phi(\theta) \equiv \phi(X_v) \quad (\pi^{v+1})$, donc $\phi(\theta) = 0$

$k_{\mathcal{U}}(\theta)$ est alors extension algébrique finie de $k_{\mathcal{U}}$ de degré n , et est contenue dans $\mathcal{K}$: donc $\mathcal{K} = k_{\mathcal{U}}(\theta)$.

$K = k(\theta)$ est extension algébrique de k de degré n , et la valeur absolue φ y définit une valuation π -adique, π étant un idéal premier de K ; l'ensemble K_{π} des limites de

nombre de K , contenant à la fois θ et $k_{\mathcal{U}}$, se confond avec $\mathcal{K}$: $\mathcal{K} = K_{\pi}$. Il est démontré que toute extension finie d'un corps $\mathcal{U}$ -adique est un corps de même nature.