LE SÉMINAIRE DE MATHÉMATIQUES 1933–1939

édition réalisée et annotée par
Michèle Audin

1. Année 1933-1934
Théorie des groupes et des algèbres

André Weil

Corps p-adiques

Séminaire de mathématiques (1933-1934), Exposé 1-H, 11 p.

<http://books.cedram.org/MALSM/SMA_1933-1934__1__H_0.pdf>

Séminaire de mathématiques 12 mars 1934
Exposé 1-H, p. 1 à 11

CORPS p-ADIQUES

par **André Weil**

1.– Corps de nombres algébriques : rappel de notions connues. Soient[1] R le corps des nombres rationnels,[2] $k = R(\theta)$ 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 $1, \theta, \theta^2, \ldots, \theta^{n-1}$, ou plus généralement de base $\xi_1, \xi_2, \ldots, \xi_n$ si les ξ_i sont n éléments de k linéairement indépendants par rapport à R ; l'élément générique de k sera ainsi :

$$\xi = x_1\xi_1 + \cdots + x_n\xi_n, \qquad x_i \in R$$

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 $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{a}$, $\alpha + \beta \in \mathfrak{a}$ ($\mathfrak{a}$ 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*. À 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* $\alpha_1, \alpha_2, \ldots, \alpha_n$ telle que tout $\alpha \in \mathfrak{a}$ soit de la forme $\alpha = m_1\alpha_1 + \cdots + m_n\alpha_n$, m_i entiers rationnels, et réciproquement. En particulier, l'idéal (1) anneau des entiers de k a une telle base $\omega_1, \omega_2, \ldots, \omega_n$. 1/2

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

Un idéal[3] $\mathfrak{p}$ est dit *premier* si $\omega\eta \equiv 0\ (\mathfrak{p})$ entraîne que $\omega \equiv 0\ (\mathfrak{p})$ ou bien $\eta \equiv 0\ (\mathfrak{p})$. 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.*[4]

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
2/3 tourner la difficulté résultant de l'apparition de tels anneaux que Hensel a introduit les nombres $\mathfrak{p}$-adiques ; on y est conduit en considérant *simultanément* les classes de restes mod. $\mathfrak{p}^n$ quel que soit n.

3.– Nombres p-adiques : 1ère définition. Soit p premier rationnel. On considère une suite d'éléments $a_1, a_2, \dots, a_h, \dots, a_n$ représentant une classe de restes mod. p^n, de telle sorte que l'on ait $a_{n+k} \equiv a_n \ (p^n)$ quels que soient n et k. Une telle suite sera appelée un *entier p-adique* A. À tout entier rationnel a correspond évidemment une telle suite, celle qu'on obtient en prenant $a_n \equiv a \ (p^n)$; la réciproque n'est pas vraie ; cette suite s'appellera l'entier p-adique a. Les entiers p-adiques forment un anneau : si :

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

on écrira :

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

Si $a_n \equiv 0 \ (p^n)$, d'où $a_{n+k} \equiv 0 \ (p^n)$ on écrira $A \equiv 0 \ (p^n)$. Si $A \equiv 0 \ (p^n)$ quel que soit n, $A = 0$: il en résulte que l'anneau des A est sans diviseur de zéro, car si $A \not\equiv 0 \ (p^m)$, $B \not\equiv 0 \ (p^n)$, on a $A \cdot B \not\equiv 0 \ (p^{m+n})$. 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 $B \not\equiv 0 \ (p)$,
3/4 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 $B \equiv 0 \ (p^n)$ et $\not\equiv 0 \ (p^{n+1})$, $B = p^n \cdot B_1$ et $B_1 \not\equiv 0 \ (p)$, donc tout nombre p-adique A/B peut s'écrire $\dfrac{C}{p^n}$, $C = A/B_1$ 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 $\varphi(\xi) \geqslant 0$ non constante, des éléments de k, telle que

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

(B) $$\varphi(\xi+\eta) \leqslant \varphi(\xi)+\varphi(\eta)$$

(On en tire aussitôt que $\varphi(0)=0$, $\varphi(\pm 1)=1$).

(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*[5] : 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 dite 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 coprs *parfait* (au sens topologique[6]), 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, 4/5
$\varphi(\Xi)$ sera $\lim\varphi(\xi_n)$ (qui existe car $|\varphi(\xi_m)-\varphi(\xi_n)|\leqslant\varphi(\xi_m-\xi_n)$ d'après (B)).

$\xi\pm\eta$ et $\xi\eta$ sont d'après (B) et (A), fonctions continues de ξ, η, au sens de la distance φ ; de même $\dfrac{1}{\xi}$ pour $\xi\neq 0$; donc si $\Xi=\lim\xi_n$, $\mathrm{H}=\lim\eta_n$, on peut définir $\Xi+\mathrm{H}$, $\Xi\mathrm{H}$ comme limites de $\xi_n\pm\eta_n$ et $\xi_n\eta_n$ respectivement. De même, $\dfrac{1}{\Xi}=\lim\dfrac{1}{\xi_n}$ 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.[7]

5.–. Mais il faut distinguer deux cas[8] : Soit d'abord (valuation de 1ère espèce), $\varphi(a)\leqslant 1$ 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 :

$$m=c_0+c_1a+\cdots+c_{k-1}a^{k-1},\qquad 0\leqslant c_i<a$$

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

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

donc $\varphi(m)\leqslant k\varphi_0$, et de même $\varphi(m^\nu)\leqslant k\nu\varphi_0$ quel que soit ν, donc $\varphi(m)\leqslant 1$.

Soient alors ξ, η dans k, et par exemple $\varphi(\xi)\leqslant\varphi(\eta)$, on a[9] : 5/6

$$\begin{aligned}\varphi[(\xi+\eta)^\nu]&=[\varphi(\xi+\eta)]^\nu\\&\leqslant\varphi(\xi^\nu)+\varphi(c_1^{\nu-1})\varphi(\xi^{\nu-1})\varphi(\eta)+\varphi(c_2^{\nu-2})\varphi(\xi^{\nu-2})\varphi(\eta^2)+\cdots\\&\leqslant(\nu+1)\varphi(\eta)^\nu\end{aligned}$$

quel que soit ν, d'où[10]

(C) $$\varphi(\xi+\eta)\leqslant\varphi(\eta)$$

Soit maintenant ω entier : $\omega = m_1\omega_1 + \cdots + m_n\omega_n$ donc par (C), $\varphi(\omega)$ est $\leqslant$ au plus grand des nombres $\varphi(\omega_1), \ldots, \varphi(\omega_n)$, donc borné, donc $\leqslant 1$, car sinon $\varphi(\omega^\nu)$ serait non borné. Considérons les ω tels que $\varphi(\omega) < 1$; il en existe, sinon φ serait constante. Ils forment un idéal d'après (C), et un idéal premier d'après (A) ; soit $\mathfrak{p}$ cet idéal, π un entier $\equiv 0$ $(\mathfrak{p})$ et $\not\equiv 0$ $(\mathfrak{p}^2)$, 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 $\mathfrak{p}^m$, avec $m \lesseqgtr 0$, ce facteur est dit la contribution de $\mathfrak{p}$ à ξ ; sinon on prend $m = 0$ et la contribution de $\mathfrak{p}$ à ξ sera 1 ; soit donc en tout cas $\mathfrak{p}^m$ cette contribution, l'expression de $\xi\pi^{-m}$ ne contient plus $\mathfrak{p}$ donc $\xi\pi^{-m}$ est quotient de deux entiers $\not\equiv 0$ $(\mathfrak{p})$; 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 $\mathfrak{p}$ et à tout $w < 1$ correspond une valuation φ. La fermeture de k par cette valuation est dite le *corps* $\mathfrak{p}$-*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 (rationnel) multiple de $\mathfrak{p}$, l'on ait $\varphi(p) = \dfrac{1}{p}$: φ est alors la *valeur*
6/7 *absolue* $\mathfrak{p}$-*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[11] :

$$\varphi(m) \leqslant \varphi_0[1 + \varphi(a) + \cdots + \varphi(a)^{k-1}] = \varphi_0 \frac{\varphi(a)^k - 1}{\varphi(a) - 1} \varphi(a)^{k\nu}$$

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

De même, quels que soient les entiers h, k tels que : $m^h < a^k$, on a $\varphi(m)^h \leqslant \varphi(a)^k$;

$$\frac{h}{k} < \frac{\log a}{\log m} \text{ entraîne } \frac{\log \varphi(a)}{\log \varphi(m)} \geqslant \frac{h}{k} \text{ donc } \frac{\log \varphi(a)}{\log \varphi(m)} \geqslant \frac{\log a}{\log m}$$

et de même

$$\frac{\log \varphi(m)}{\log \varphi(a)} \geqslant \frac{\log m}{\log a} \text{ et par suite } \varphi(a) = |a|^\lambda \quad \lambda = \mathrm{C^{te}}.$$

D'ailleurs, par (B),

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

Réciproquement, $\varphi(x) = |x|^\lambda$ fournit, quel que soit $\lambda \leqslant 1$, une valuation du corps R, sa fermeture Ω étant le corps des nombres réels. Si k est quelconque, il contient en tout cas R, et sa fermeture contient Ω (plus exactement, un corps isomorphe à Ω). 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, $\varphi(\xi) = |\xi_1|^\lambda$, à tout corps k_1 et à tout $\lambda \leqslant 1$ correspond une valuation de k. Si k n'est pas dans Ω, formons dans la fermeture de k le plus petit corps $k \cdot \Omega$ qui contienne à la fois k et Ω : c'est une extension finie de Ω, donc isomorphe au corps des nombres complexes ; soit, dans
7/8 ce corps, l'élément $z = e^{i\theta}$; $\varphi(z^\nu) = \varphi(\cos\nu\theta + i\sin\nu\theta) \leqslant |\cos\nu\theta|^\lambda + \varphi(i) \cdot |\sin\nu\theta|^\lambda$ sera borné quel que soit $\nu \lesseqgtr 0$, donc $\varphi(e^{i\theta}) = 1$; et par suite, z étant un nombre

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, et à $\lambda \leqslant 1$ 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. Il semblerait donc qu'il y ait n familles de valuations de k_1, mais en réalité deux corps k_1, imaginaires conjugués, donnent 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 $\mathfrak{p}$-adiques. l'analyse dans ces corps repose sur le fait suivant, conséquence immédiate de (C) : *Pour que la série* $\sum_1^\infty \Xi_n$ *converge, il faut et il suffit que* Ξ_n *tende vers* 0.

Parmi les Ξ, on distingue les entiers $\mathfrak{p}$-adiques Ω, limites d'entiers de k. Pour un tel nombre, on a $\varphi(\Omega) \leqslant 1$. Réciproquement, soit $\Omega = \lim \xi_n$ et $\varphi(\Omega) \leqslant 1$; pour n assez grand, $\varphi(\xi_n) \leqslant 1$, donc $\xi_n = \dfrac{\omega_n}{\eta_n}$, ω_n et η_n étant entiers et $\eta_n \not\equiv 0\ (\mathfrak{p})$; on pourra alors 8/9
trouver ω'_n entier tel que $\omega_n \equiv \eta_n \omega'_n\ (\mathfrak{p}^n)$ et Ω sera limite des ω'_n.

Les entiers $\mathfrak{p}$-adiques forment *un anneau*. À tout Ω entier correspond, quel que soit n, une classe de restes mod. $\mathfrak{p}^n$ 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. prg.3). L'inverse d'un entier $E \not\equiv 0\ (\mathfrak{p})$ est encore entier : car si $E = \lim \omega_n$, $\omega_n \not\equiv 0\ (\mathfrak{p})$ et on aura $1/E = \lim \eta_n$, les entiers η_n étant tels que $\omega_n \eta_n \equiv 1\ (\mathfrak{p}^n)$. Ces entiers s'appellent *unités* $\mathfrak{p}$-*adiques* ; ce sont les nombres pour lesquels $\varphi(E) = 1$. Si $\varphi(\Xi) = w^m$, on aura $\Xi = \pi^m E$, E étant une unité.

Les entiers $\equiv 0\ (\mathfrak{p})$ forment, dans l'anneau des entiers $\mathfrak{p}$-adiques, un *idéal premier*, qui s'appellera encore l'idéal $\mathfrak{p}$. *Tout idéal dans l'anneau est puissance de* $\mathfrak{p}$: 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 $\geqslant m$, et par hypothèse ceux-là seulement : il se confond avec $\mathfrak{p}^m$. De plus, *tout idéal est un idéal principal* : car $\mathfrak{p}^m = (\pi^m) = (\pi^m E)$, E étant une unité quelconque.

Prenons des entiers $\mathfrak{p}$-adiques formant un système complet de restes mod. $\mathfrak{p}$: nous pouvons par exemple choisir pour cela des entiers de k, $\xi_1, \xi_2, \ldots, \xi_q$ (d'ailleurs $q =$ norme de $\mathfrak{p} = p^F$, F étant le degré de $\mathfrak{p}$). Soit Ξ un entier quelconque, il sera congru 9/10
mod. $\mathfrak{p}$ à l'un des ξ, soit ξ_{i_0} ; $\dfrac{\Xi - \xi_{i_0}}{\pi}$ sera alors entier, et $\equiv \xi_{i_1}\ (\mathfrak{p})$. Soit donc en général : $\Xi_n = \dfrac{\Xi_{n-1} - \xi_{i_{n-1}}}{\pi} \equiv \xi_{i_n}\ (\mathfrak{p})$; Ξ pourra s'exprimer par un développement

en série convergente suivant les puissances de π :

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

et l'on obtiendra tous les entiers $\mathfrak{p}$-adiques une fois et une seule en donnant aux coefficients les q valeurs incongrues mod. $\mathfrak{p}$ (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 :

$$\Xi = \sum_{\nu=0}^{\infty} \xi_{i_\nu}\pi^{-m+\nu}$$

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 un 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. $\mathfrak{p}$: ils forment une suite partielle, d'où l'on peut à nouveau extraire une suite d'entiers qui ont même reste mod. $\mathfrak{p}^2$ et ainsi de suite. La suite diagonale est alors convergente.

8.– Théorie des extensions finies. Soit $k_\mathfrak{p}$ le corps $\mathfrak{p}$-adique déduit de k et de
10/11 l'idéal premier $\mathfrak{p}$ dans k, p étant le nombre premier $\equiv 0$ $(\mathfrak{p})$, les limites de nombres rationnels forment dans $k_\mathfrak{p}$ un sous-corps R_p qui n'est autre que le corps des nombres p-adiques. $k_\mathfrak{p}$ est *extension algébrique finie de* R_p : soit, en effet, Ξ un nombre de $k_\mathfrak{p}$: pour m assez grand, $p^m\Xi = \Omega$ sera un entier limite d'une suite d'entiers $\omega = m_1\omega_1 + m_2\omega_2 + \cdots + m_n\omega_n$ 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 :

$$\Omega = M_1\omega_1 + \cdots + M_n\omega_n$$
$$\text{et } \Xi = X_1\omega_1 + X_2\omega_2 + \cdots + X_n\omega_n,$$

les X_i étant des nombres de R_p : $k_\mathfrak{p}$ est donc un R_p-module fini, donc, comme on sait, une extension algébrique finie, de degré $\leqslant n$. Avec les notations des systèmes hypercomplexes, on peut écrire[12] $k_\mathfrak{p} = k \times R_p$

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_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 polynome irréductible dans le corps $\mathfrak{p}$*-adique* $k_\mathfrak{p}$ *est irréductible ou puissance de*
11/12 *polynomes irréductibles modulo* $\mathfrak{p}$.

Soit en effet $F(x)$ un polynome de degré n à coefficients $\mathfrak{p}$-adiques : montrons que si $F(x) \equiv f(x)\cdot g(x)$ $(\mathfrak{p})$, f et g étant deux polynomes premiers entre eux mod. $\mathfrak{p}$, F ne peut être irréductible. Soient r, s, les degrés de f et g (avec $r+s=n$). On pourra

déterminer par récurrence des polynomes f_n et g_n de degrés r, s, de sorte que l'on ait :

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

car si on pose

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

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

$$\pi^n(\varphi_{n-1} g_n + \psi_{n-1} f_n) \equiv F - \varphi_{n-1}\psi_{n-1} \ (\mathfrak{p}^{n+1})$$

c'est à dire :

$$f g_n + g f_n \equiv \frac{F - \varphi_{n-1}\psi_{n-1}}{\pi^n} \ (\mathfrak{p})$$

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 polynomes $\mathfrak{p}$-adiques de degrés r, s, d'ailleurs premiers entre eux.

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

Soit H un élément de $\mathfrak{K}$: H et ses conjugués $\mathrm{H}', \mathrm{H}'', \ldots, \mathrm{H}^{(n-1)}$ seront les racines d'une équation *normée* (coefficient de $x^n = 1$) bien déterminée à coefficients dans $k_\mathfrak{p}$ 12/13
et H sera dit *entier* si ces coefficients sont des entiers de $k_\mathfrak{p}$. Soit nH la norme de H, c'est à dire $(-1)^n\times$ le terme constant de cette équation. Posons $\varphi(\mathrm{H}) = [\varphi(n\mathrm{H})]^{\frac{1}{n}}$: si H est dans $k_\mathfrak{p}$, cette fonction coïncide bien avec la valeur absolue. Évidemment $\varphi(\mathrm{H} \cdot \mathrm{H}_1) = \varphi(\mathrm{H}) \cdot \varphi(\mathrm{H}_1)$. Démontrons les deux théorèmes suivants :

1. *Pour que* H *soit entier, il faut et il suffit que* $\varphi(\mathrm{H})$ *soit* $\leqslant 1$*, c'est à dire que* nH *soit entier.*

2. *Si* $\varphi(\mathrm{H}) \leqslant \varphi(\mathrm{H}_1)$*,* $\varphi(\mathrm{H} + \mathrm{H}_1) \leqslant \varphi(\mathrm{H}_1)$.

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 $\equiv x^r \cdot g(x)$ $(\mathfrak{p})$, x^r et $g(x)$ étant premiers entre eux mod. $\mathfrak{p}$ (et $r > 0$). $F(x)$ serait donc, d'après la démonstration du lemme, produit de deux polynomes premiers entre eux, ce qui est impossible ; par suite, $k = 0$ et H est entier.

2. On aura $\varphi\left(\dfrac{\mathrm{H}}{\mathrm{H}_1}\right) \leqslant 1$, donc $\dfrac{\mathrm{H}}{\mathrm{H}_1}$ est entier, donc $1 + \dfrac{\mathrm{H}}{\mathrm{H}_1}$ l'est aussi, et $\varphi\left(1 + \dfrac{\mathrm{H}}{\mathrm{H}_1}\right) \leqslant 1$.

On peut alors étendre au corps $\mathfrak{K}$ toute la théorie exposée aux parg.5 et 7 pour les corps $\mathfrak{p}$-adiques. Remarquons en effet que, si l'on pose $w = \varphi(\pi)$, $\log \varphi(\mathrm{H})$ est toujours un multiple entier de $\frac{1}{n}\log\frac{1}{w}$; et appelons $\log\frac{1}{W}$ la plus petite valeur de $|\log\varphi(\mathrm{H})|$;
13/14 soit Π un élément de $\mathfrak{K}$ tel que $\varphi(\Pi) = W$, l'idéal principal $(\Pi) = \mathcal{P}$ sera l'unique idéal premier de l'anneau des entiers de $\mathfrak{K}$, et tous les idéaux de cet anneau seront des puissances de $\mathcal{P}$: en particulier, pour l'idéal (π) de cet anneau que nous appellerons encore $\mathfrak{p}$, on aura $\mathfrak{p} = \mathcal{P}^e$.

Enfin, l'anneau des entiers de $\mathfrak{K}$ est un module fini, de rang n, par rapport à l'anneau des entiers de $k_\mathfrak{p}$; on le démontre en déterminant une base $\mathrm{H}_1, \mathrm{H}_2, \ldots, \mathrm{H}_n$, 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. $\mathcal{P}$ dans $\mathfrak{K}$ est un module de rang fini $f \leqslant n$ par rapport au corps des classes de restes mod. $\mathfrak{p}$ dans $k_\mathfrak{p}$; il y a un nombre fini d'éléments, et comme il est sans diviseurs de zéros, c'est un corps fini (champ de Galois). De là, on déduit, pour $\mathfrak{K}$ 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 de classes de restes mod. $\mathfrak{p}$ dans $k_\mathfrak{p}$, q^f sera le nombre de classes de restes mod. $\mathcal{P}$ dans $\mathfrak{K}$; le nombre de classes de restes mod. $\mathcal{P}^e = \mathfrak{p}$ dans $\mathfrak{K}$ sera alors $(q^f)^e$, comme on le voit par exemple au moyen du développement suivant les puissances de Π. Mais d'autre part, $\mathrm{H}_1, \mathrm{H}_2, \ldots, \mathrm{H}_n$ forment une base des entiers de $\mathfrak{K}$, par rapport à l'anneau des entiers de $k_\mathfrak{p}$, tout entier H de
14/15 $\mathfrak{K}$ est de la forme $\sum_{i=1}^{n} \xi_i \mathrm{H}_i$, les ξ_i étant des entiers de $k_\mathfrak{p}$: on obtient toutes les classes de restes mod. $\mathfrak{p}$ dans $\mathfrak{K}$ en donnant à chacun des ξ_i q valeurs incongrues mod. $\mathfrak{p}$ et on obtient chacune une fois et une seule, car si $\sum \xi_i \mathrm{H}_i \equiv \sum \xi'_i \mathrm{H}_i$ $(\mathfrak{p})$, $\sum \frac{\xi_i - \xi'_i}{\pi}\mathrm{H}_i$ est entier, donc $\xi_i \equiv \xi'_i$ $(\mathfrak{p})$. Il y a donc dans $\mathfrak{K}$, q^n classes de restes mod. $\mathfrak{p}$; et par suite $n = e \cdot f$; f s'appelle *le degré relatif* de $\mathcal{P}$ par rapport à $k_\mathfrak{p}$, *e l'ordre de ramification* de $\mathfrak{p}$ dans $\mathfrak{K}$.

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

de degré f de $k_\mathfrak{p}$, $\mathfrak{K}$ est extension algébrique de degré $\dfrac{n}{f} = e$ de $\overline{k}_{\overline{\mathfrak{p}}}$. Mais le corps 15/16
des classes de restes mod. $\overline{\mathfrak{p}}$ dans $\overline{k}_{\overline{\mathfrak{p}}}$ est contenu dans $\mathfrak{K}^\star$, contient $k^\star$, et contient une racine $\eta^\star$ de $F(x) = 0$, il est donc de degré f par rapport à $k^\star$, et se confond avec $\mathfrak{K}^\star$. Par suite, le degré relatif de l'idéal $\mathcal{P}$ par rapport à $\overline{k}_{\overline{\mathfrak{p}}}$ est 1 ; celui de de $\overline{\mathfrak{p}}$ par rapport à k est f, et puisque f est aussi le degré $\overline{n}$ de $\overline{k}_{\overline{\mathfrak{p}}}$ par rapport à $k_\mathfrak{p}$, l'ordre de ramification $\overline{e} = \dfrac{\overline{n}}{f}$ de $\mathfrak{p}$ dans $\overline{k}_{\overline{\mathfrak{p}}}$ est 1, on peut écrire $\overline{\mathfrak{p}} = \mathfrak{p}$.

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

11.–. Pour achever de démontrer que $\mathfrak{K}$ peut être considéré comme corps $\mathfrak{p}$-adique, prenons $\overline{k}$ comme point de départ, et pour simplifier les notations, appelons le désormais k. Cela revient à supposer que $f = 1$ et $e = n$. Soit $\mathfrak{K} = k_\mathfrak{p}(\theta)$, 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 polynomes φ, ψ à coefficients entiers dans $k_\mathfrak{p}$, tels que $\Phi_0(X) \equiv \varphi(X) \cdot \psi(X)$ $(\mathfrak{p}^\mu)$; sinon, en effet, on pourrait trouver une suite de valeurs de μ indéfiniment croissantes tels [telles]que les polynomes φ, ψ correspondants convergent et Φ_0 ne sera pas irréductible. Dans ces 16/17
conditions, tout polynome $\Phi(X)$ congru à Φ_0 mod. $\mathfrak{p}^\mu$ sera irréductible dans $k_\mathfrak{p}$; car sinon (en vertu d'un raisonnement bien connu) il serait produit de deux polynomes φ, ψ à coefficients entiers.

Supposons alors que $\Phi_0'(\theta)$ soit $\equiv 0$ $(\mathcal{P}^{r-1})$ et $\not\equiv 0$ $(\mathcal{P}^r)$. On peut toujours écrire $\theta = \xi_0 + \xi_1\Pi + \cdots + \xi_{r-1}\Pi^{r-1} + \theta'\Pi^r$ les ξ_s étant des entiers pris par exemple dans k, et θ' étant entier. Prenons un polynome $\Phi(X)$ *à coefficients dans* k et $\equiv \Phi_0(X)$ $(\mathfrak{p}^\alpha)$, α étant $\geqslant 2r$ et $\geqslant \mu$.

Nous allons montrer que l'on peut déterminer par récurrence $\xi_r, \xi_{r+1}, \ldots$ de façon que :

$$\theta = \xi_0 + \xi_1\Pi + \cdots + \xi_{r-1}\Pi^{r-1} + \xi_r\Pi^r + \xi_{r+1}\Pi^{r+1} + \cdots$$

soit racine de $\Phi(X) = 0$. Posons pour cela :

$$X_\nu = \xi_0 + \xi_1\Pi + \cdots + \xi_\nu\Pi^\nu$$

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

$$0 = \Phi_0(\theta) \equiv \Phi_0(X_{r-1}) + \Phi_0'(X_{r-1}) \cdot \theta'\Pi^r \quad (\mathcal{P}^{2r})$$

d'ailleurs $\Phi_0'(X_{r-1}) \equiv \Phi_0'(\theta)$ $(\mathcal{P}^r)$, donc :

$$\Phi_0'(X_{r-1}) \equiv 0 \quad (\mathcal{P}^{r-1}), \text{ et}$$
$$\Phi_0(X_{r-1}) \equiv 0 \quad (\mathcal{P}^{2r-1})$$

par suite, aussi, $\Phi(X_{r-1}) \equiv 0$ $(\mathcal{P}^{2r-1})$ puisque $\Phi \equiv \Phi_0$ $(\mathcal{P}^{2r})$. De plus, $\Phi'(X_{r-1}) \equiv \Phi'_0(X_{r-1})$ $(\mathcal{P}^{2r})$, donc $\Phi'(X_{r-1})$ est $\equiv 0$ $(\mathcal{P}^{r-1})$ et $\not\equiv 0$ $(\mathcal{P}^r)$.

Supposons que l'on ait déterminé $\xi_r, \xi_{r+1}, \dots, \xi_{\nu-1}$ $(\nu \geqslant r)$ de telle sorte que
17/18 $\Phi(X_{\nu-1}) \equiv 0$ $(\mathcal{P}^{\nu+r-1})$ et que $\Phi'(X_{\nu-1})$ soit $\equiv 0$ $(\mathcal{P}^{r-1})$ et $\not\equiv 0$ $(\mathcal{P}^r)$; nous venons de voir qu'il en est bien ainsi pour $\nu = r$.

Soit $X_\nu = X_{\nu-1} + \xi_\nu \Pi^\nu$, on aura :

$$\Phi(X_\nu) \equiv \Phi(X_{\nu-1}) + \Phi'(X_{\nu-1})\xi_\nu \Pi^\nu \quad (\mathcal{P}^{2\nu})$$

donc on pourra développer ξ_ν par la condition :

$$\xi_\nu \equiv -\frac{\Phi(X_{\nu-1})}{\Phi'(X_{\nu-1})\Pi^\nu} \quad (\mathcal{P});$$

le second membre est entier, on peut prendre pour ξ_ν par exemple un entier de k. On aura bien $\Phi(X_\nu) \equiv 0$ $(\mathcal{P}^{\nu+r})$, et $\Phi'(X_\nu)$ sera $\equiv 0$ $(\mathcal{P}^{r-1})$ et $\not\equiv 0$ $(\mathcal{P}^r)$. En poursuivant ainsi on déterminera θ comme somme d'une série convergente ; et $\Phi(\theta) \equiv \Phi(X_\nu)$ $(\mathcal{P}^{\nu+1})$, donc $\Phi(\theta) = 0$.

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

$K = k(\theta)$ est extension algébrique de k de degré n et la valeur absolue φ y définit une valuation $\mathcal{P}$-adique, $\mathcal{P}$ étant un idéal premier de K ; l'ensemble $K_\mathcal{P}$ des limites de nombres de K, contenant à la fois θ et $k_\mathfrak{p}$, se confond avec $\mathfrak{K}$: $\mathfrak{K} = K_\mathcal{P}$. Il est démontré que toute extension finie d'un corps $\mathfrak{p}$-adique est un corps de même nature.

Notes

1. Les références bibliographiques de cet exposé figurent à la fin du suivant (ce sont [Hen18, Has31, Art32, Che33]).
2. Les notations aujourd'hui standard pour les ensembles de nombres n'étaient pas fixées.
3. La lettre utilisée par Weil est un p gothique et manuscrit (elle est d'ailleurs manuscrite).
4. L'anneau des entiers d'un corps de nombres est un anneau de Dedekind.
5. Les notions sont clairement définies. Une suite convergente est ce que nous appelons aujourd'hui une suite de Cauchy. Elle peut avoir (ou ne pas avoir) une limite.
6. Un espace topologique est parfait s'il n'a pas de point isolé.
7. Quatre ans plus tard, dans les exposés 5-C et D, Chevalley utilisera les structures uniformes, tout juste inventées par Weil [Wei37], pour montrer la complétude.
8. Cette démonstration, aujourd'hui classique, d'un théorème d'Ostrowski [Ost17], est due à Emil Artin [Art32].
9. Dans ces formules, c_i^j désigne le coefficient binomial $\binom{i+j}{i}$.
10. en prenant les racine ν-ièmes et en faisant tendre ν vers $+\infty$
11. Le facteur $\varphi(a)^{k\nu}$ dans la ligne suivante semble une erreur. La démonstration est un peu concise. Des propriétés de la valuation, il suit que $\varphi(1) = 1$ et que pour tout $a \in \mathbf{Z}$,

$\varphi(a) \leqslant |a|$. D'où l'on tire, en écrivant m en base a,

$$\varphi(m) \leqslant \sqrt[\nu]{a\left(\frac{\nu \log m}{\log a}+1\right)\max(1, \varphi(m)^{\nu \log m/\log m})}$$

puis, en faisant tendre ν vers $+\infty$,

$$\varphi(m) \leqslant \max(1, \varphi(a)^{\log m/\log a}).$$

Dans le cas considéré, on a $\varphi(m) > 1$ et $\varphi(a)$ aussi. On obtient

$$\varphi(m)^{1/\log m} \leqslant \varphi(a)^{1/\log a}$$

qui devient une égalité puisqu'on peut y échanger les rôles de a et m. On en déduit que $\varphi(x) = |x|^\rho$ pour un $\rho \in]0, 1]$.

12. Les « notations des systèmes hypercomplexes » sont celles dans lesquelles $\times$ désigne le produit tensoriel.

Des archives du séminaire...

Compte-rendu de la séance du 12 Mars 1934

1. M.JULIA étant en mission à Rome, c'est M.CARTAN qui préside et ouvre la séance à 16h.30.

2. Il donne la parole à Weil, qui fait un premier exposé sur l'Arithmétique p-adique.

3. Après l'exposé de Weil, quelques questions lui sont posées. Thé. Conversations. La séance est levée à 18h.15 [1].

Références

[Art32] E. Artin – « Über die Bewertungen algebraischer Zahlkörper », *J. Reine Angew. Math.* **167** (1932), p. 157–159.

[Che33] C. Chevalley – « Sur la théorie du corps de classes dans les corps finis et les corps locaux. », *J. Fac. Sci. Univ. Tokyo, Sect. I* **2** (1933), p. 365–476.

[Has31] H. Hasse – « Über $\mathfrak{p}$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme », *Math. Ann.* **104** (1931), p. 495–534.

[Hen18] K. Hensel – « Eine neue Theorie der algebraischen Zahlen », *Math. Z.* **2** (1918), p. 433–452.

[Ost17] A. Ostrowski – « Über einige Lösungen der Funktionalgleichung $\varphi(x) \cdot \varphi(y) = \varphi(xy)$ », *Acta Math.* **41** (1917), p. 271–284.

[Wei37] A. Weil – *Sur les espaces à structure uniforme et sur la topologie générale*, Publications de l'Institut de mathématiques de l'université de Strasbourg, Hermann, Paris, 1937.

1. Une page ronéotypée, archives de l'IHP.