Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Yvette Dejean

Fonction exponentielle dans un corps p-adique

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 2 (1960-1961), exp. n° 10, p. 1-8

<http://www.numdam.org/item?id=SDPP_1960-1961__2__A10_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
2e année, 1960/61, n° 10

20 mars et 17 avril 1961

FONCTION EXPONENTIELLE DANS UN CORPS p-ADIQUE

par Mme Yvette DEJEAN

NOTATIONS. - Nous supposerons $p \neq 2$. $\mathfrak{k}$ étant un corps local de degré n sur $\mathbb{Q}_p$, nous noterons : $\mathfrak{p}$, l'idéal maximal de $\mathfrak{k}$, engendré par un élément π . Pour $x \in \mathfrak{k}$, $\lambda(x)$ sera l'ordre de x , normalisé par $\lambda(p) = 1$, donc $\lambda(\pi) = \frac{1}{e}$ (e = exposant de $\mathfrak{k} = \frac{n}{f}$, f = norme de $\mathfrak{k}$).

L'exponentielle et le logarithme étant définis par les séries habituelles, nous chercherons à les étendre hors des cercles de convergence de ces séries, en utilisant les relations fonctionnelles :

$$\exp(x_1 + x_2) = (\exp x_1).(\exp x_2) \tag{1}$$

$$\mathrm{Log}(x_1\, x_2) = \mathrm{Log}\, x_1 + \mathrm{Log}\, x_2 \quad . \tag{2}$$

Nous définirons ainsi, pour tout $x \in \mathbb{Q}_p$ une exponentielle multiforme à valeurs dans des extensions algébriques de $\mathbb{Q}_p$, et pour toute unité de certains corps locaux $\mathfrak{k}$, un logarithme à valeurs dans $\mathfrak{k}$.

1. La série exponentielle.

Lorsque la série

$$1 + \frac{x}{1!} + \ldots + \frac{x^n}{n!} + \ldots \tag{3}$$

est convergente pour $x = x_1$, x_2 et $x_1 + x_2$, sa somme, exp x , vérifie la relation (1).

a. Convergence. - On sait que (3) converge pour

$$\boxed{\lambda(x) > \frac{1}{p-1}} \quad .$$

En effet, si $n = a_0 + a_1 p + \ldots + a_h p^h$ ($0 \leq a_i < p$, $a_i \in \mathbb{Z}$)

$$\lambda(n!) = \frac{1}{p-1}\,[n - (a_0 + a_1 + \ldots + a_h)] \quad .$$

Alors

$$\lambda(\frac{x^n}{n!}) = n(\lambda(x) - \frac{1}{p-1}) + \frac{a_0 + \dots + a_h}{p-1} \quad .$$

Lorsque $n = p^\mu$ ($\mu > 0$, $\mu \in \underset{\sim}{Z}$) ; $\frac{a_0 + \dots + a_h}{p-1} = \frac{1}{p-1}$, donc pour que $\lambda(\frac{x^n}{n!}) \to +\infty$ avec n , il faut et il suffit que $\lambda(x) > \frac{1}{p-1}$.

Pour $x \in \underset{\sim}{Q}_p$, $\lambda(x) > \frac{1}{p-1} \iff \lambda(x) \geqslant 1 \iff x \in (p)$.

b. Valeurs prises. - Si $x \in (p)$, $\exp x \equiv 1 \pmod p$, en effet $\lambda(\frac{x^n}{n!}) \geqslant 1$ pour $n \geqslant 1$. De plus

$$\boxed{\exp x \equiv 1 + x \pmod{p^{\lambda(x)+1}}} \quad . \tag{4}$$

En effet

$$\lambda(\frac{x^n}{n!}) \geqslant n(\lambda(x) - \frac{1}{p-1}) + \frac{1}{p-1} \quad \text{pour} \quad n \geqslant 1$$

donc

$$\lambda(\frac{x^n}{n!}) - \lambda(x) \geqslant (n-1)(\lambda(x) - \frac{1}{p-1}) > 0 \quad \text{pour} \quad n \geqslant 2 \quad .$$

Pour $x \in (p)$, $\exp x \in 1 + (p)$.

c. Fonction inverse. - Soit réciproquement $y = 1 + u \in 1 + (p)$, nous allons construire un $x \in (p)$ tel que $\exp x = y$ (il n'existe qu'un tel x , car $\exp x = 1$ et (4) $\Longrightarrow x = 0$). Posons

$$E = \exp p = 1 + p + \frac{p^2}{2!} + \dots + \frac{p^n}{n!} + \dots$$

Si $x \in (p)$, $x = p(a_1 + a_2 p + \dots + a_n p^{n-1} + \dots)$, $0 \leqslant a_i < p$,

$$\exp x \equiv E^{a_1 + a_2 p + \dots + a_n p^{n-1}} \pmod{p^{n+1}}$$

en effet le quotient de ces deux nombres est $\exp(a_{n+1} p^{n+1} + \dots) \equiv 1 + a_{n+1} p^{n+1} \pmod{p^{n+2}}$. Donc le produit infini

$$E^{a_1} . E^{a_2 p} \dots E^{a_n p^{n-1}} \dots = E^{x/p}$$

est convergent, et

$$\exp x = E^{x/p} \quad .$$

Soit $y = 1 + u_1 p + \ldots + u_n p^n + \ldots \in 1 + (p)$, $0 \leq u_i < p$.

Il existe un a_1 , $0 \leq a_1 < p$, unique, tel que $y \equiv E^{a_1} \pmod{p^2}$, c'est $a_1 = u_1$.

Soit $y_1 = \dfrac{y}{E^{a_1}} = 1 + u_2^1 p^2 + \ldots$. Si $a_2 = u_2^1$, $y_1 \equiv E^{a_2 p} \pmod{p^3}$.

On construirait ainsi par récurrence une suite $a_1 , a_2 , \ldots , a_n , \ldots$, $0 \leq a_i < p$, telle que

$$y \equiv E^{a_1 + a_2 p + \ldots + a_n p^{n-1}} \pmod{p^{n+1}}$$

et le nombre $x = a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots$ est tel que $\exp x = E^{x/p} = y$.

Nous avons donc un procédé de calcul pour $x = \operatorname{Log} y$, $\forall$ $y \in 1 + (p)$.

d. Continuité. - Elle résulte de la convergence uniforme de (3) dans le disque $|x| \leq \frac{1}{p}$, ou encore de la continuité à l'origine, évidente d'après (4).

En résumé, la série (3) réalise une représentation continue biunivoque du groupe additif (p) sur le groupe multiplicatif $1 + (p)$.

2. Prolongement pour $x \notin (p)$.

Soit $x \notin (p)$, la série (3) ne permet pas de définir $\exp x$. Si $\mu = - \lambda(x) + 1$, $\mu \in \underset{\sim}{Z}$, $\mu \geq 1$, $p^\mu x \in (p)$ et $\exp(p^\mu x)$ est défini par (3) . Une exponentielle prolongeant (3) est nécessairement telle que

$$(\exp x)^{p^\mu} = \exp p^\mu x = y \in 1 + (p) \quad .$$

Donc le prolongement de (3) à la boule $|x| \leq p^{\mu-1}$ est ramené à la résolution de l'équation

$$E_\mu(y) \qquad \boxed{\eta^{p^\mu} = y} \quad , \quad \forall \quad y \in 1 + (p)$$

a. Série $(1 + u)^{1/p^\mu}$. - Lorsque la série

(5) $$1 + \sum_{n=1}^{+\infty} c_n u^n \ , \quad c_n = (-1)^{n-1} \frac{(p^\mu - 1)(2p^\mu - 1) \dots ((n-1)p^\mu - 1)}{p^{n\mu} n!}$$

converge, pour $u = y - 1$, sa somme est une solution de $E\mu$.

Or $\lambda(c_n) = -n\mu - \frac{n}{p-1} + \frac{1}{p-1}[a_0 + a_1 + \dots + a_h]$ (notations du (1. a)). Donc pour que (5) converge il faut et il suffit que

$$\lambda(u) > \mu + \frac{1}{p-1} \ , \text{ soit } \lambda(u) \geqslant \mu + 1 \geqslant 2 \quad .$$

Lorsque $y = \exp(p^\mu x)$ avec $\mu = -\lambda(x) + 1$, $\lambda(y-1) = 1$ et la série (5) ne nous permet pas de prolonger l'exponentielle hors de (p) .

b. Nécessité d'étendre $\underset{\sim}{Q}_p$. - Nous allons montrer que $\underset{\sim}{Q}_p$ ne contient aucune racine de E_μ lorsque $\lambda(y-1) = 1$. En effet si η est une telle racine, soit $z = \eta - 1$, z est une racine de

$$(z+1)^{p^\mu} = y \ , \quad \text{donc} \quad N(z) = y - 1 \quad \text{et} \quad \lambda(z) = \frac{1}{p^\mu}$$

ce qui prouve que $z \notin \underset{\sim}{Q}_p$ et $\eta = 1 + z$ non plus.

Construisons donc une extension $\mathfrak{k}_\mu$ de $\underset{\sim}{Q}_p$ dans laquelle E_μ aie au moins une racine quel que soit $y \in 1 + (p)$.

c. Construction de $\mathfrak{k}_\mu$. - Nous avons démontré que tout $y \in 1 + (p)$ a un logarithme $x \in (p)$, tel que

$$y = E^{x/p} \quad .$$

Soit ε_μ une racine de l'équation $x^{p^\mu} = E$.

Soit $\mathfrak{k}_\mu = \underset{\sim}{Q}_p(\varepsilon_\mu)$, $\mathfrak{k}_\mu$ est de degré p^μ car $\lambda(\varepsilon_\mu - 1) = \frac{1}{p^\mu}$.

1° $\mathfrak{k}_\mu$ ne contient aucune autre racine p^μ-ième de E . - En effet soit ε'_μ une autre racine, et $\omega_\mu = \frac{\varepsilon_\mu}{\varepsilon'_\mu} \neq 1$, ω_μ est une racine de l'équation

$$\frac{\omega^{p^\mu} - 1}{\omega - 1} = 0$$

si ce dernier polynôme n'est pas irréductible, ω est racine d'une équation de degré inférieur

$$\frac{\omega^{p^\nu} - 1}{\omega - 1} = 0 \ , \quad \nu < \mu \quad .$$

Soit ν_0 le plus grand ν ainsi obtenu, et tel que le polynôme $\frac{\omega^{p^{\nu_0}} - 1}{\omega - 1}$ soit irréductible.

Si $\nu_0 \neq 0$, ω est de degré $p^{\nu_0} - 1$ sur $\underset{\sim}{Q}_p$, et $(p^{\nu_0} - 1, p^\mu) = 1$, donc ω ne peut appartenir à $\mathfrak{k}_\mu$.

Si $\nu_0 = 0$, $\omega^{p-1} + \ldots + 1 = 0$ est réductible, ce qui est impossible si p est premier. Donc $\mathfrak{k}_\mu$ ne contient aucune racine p^ν-ième de l'unité, $\nu \leq \mu$, autre que 1.

2° $\mathfrak{k}_\mu$ contient une racine de E_μ, $\forall\ y \in 1 + (p)$. - Soit en effet $x = \operatorname{Log} y = a_1 p + \ldots + a_n p^n + \ldots$

Posons $\eta = \varepsilon_\mu^{x/p} = \varepsilon_\mu^{a_1} \ldots \varepsilon_\mu^{a_n p^n} \ldots$ [ce produit infini est convergent car $\lambda(\varepsilon_\mu - 1) = \frac{1}{p^\mu}$, donc $\varepsilon_\mu^{a_n p^n} \equiv 1 \pmod{p^{(n+1)/p^\mu}}$].

Alors η est une racine de E_μ, car $\eta^{p^\mu} = \varepsilon_\mu^{p^\mu (x/p)} = E^{x/p} = y$.

Le même raisonnement qu'au 1° montre que c'est la seule racine de E_μ que contient $\mathfrak{k}_\mu$.

d. Valeurs prises dans $\mathfrak{k}_\mu$. - Il est clair que l'exponentielle construite pour $|x| \leq p^{\mu-1}$, définie en résumé par

$$\exp x = \varepsilon_\mu^{(p^{\mu-1}x)} \quad \text{où} \quad \varepsilon_\mu^{p^\mu} = E$$

est une représentation continue du sous-groupe additif $|x| \leq p^{\mu-1}$ de $\underset{\sim}{Q}_p$ dans le sous-groupe multiplicatif $1 + \mathfrak{p}$ de $\mathfrak{k}_\mu$ ($\mathfrak{p} = (\pi_\mu)$, π_μ étant un générateur quelconque, par exemple $\pi_\mu = \varepsilon_\mu - 1$).

Ce n'est pas une représentation sur, par exemple il n'existe aucun entier n tel que $1 + \pi_\mu^2 \equiv \varepsilon_\mu^n \pmod{\pi_\mu^3}$, donc $1 + \pi_\mu^2$ n'est l'exponentielle d'aucun $x \in \underset{\sim}{Q}_p$. On peut cependant définir pour toute unité de $\mathfrak{k}_\mu$ un logarithme à valeurs dans $\mathfrak{k}_\mu$.

3. Logarithme.

Nous disposons de deux méthodes pour le définir dans $\underset{\sim}{Q}_p$:

- la construction du (1. c),

- la série

$$\text{(6)} \qquad \mathrm{Log}(1+u) = u + \frac{u^2}{2} + \ldots + \frac{u^n}{n} + \ldots$$

lorsqu'elle converge.

Or $\lambda(\frac{u^n}{n}) = n(\lambda(u) - \frac{\lambda(n)}{n})$, soit

$$n\lambda(u) \geqslant \lambda(\frac{u^n}{n}) \geqslant n[\lambda(u) - \frac{1}{\mathrm{Log}\ p} \cdot \frac{\mathrm{Log}\ n}{n}] \quad .$$

Pour que (6) converge, il faut et il suffit que $\lambda(u) > 0$, soit que $u \in (p)$. Lorsque $y = 1 + u \in 1 + (p)$, $\mathrm{Log}\ y \in (p)$ et $\exp \mathrm{Log}\ y = y$.

La série (6) définit donc pour $y \in 1 + (p)$ une fonction inverse de la série (3), nous avons au (1. c) construit cette fonction inverse et montré son unicité, donc la série (6) et le procédé du (1. c) définissent, pour tout $y \in 1 + (p)$ la même fonction $\mathrm{Log}\ y$, à valeurs dans (p) .

a. Prolongement au cercle unité. - Soit $\omega \in \underset{\sim}{Q}_p$ une racine de l'unité ($\omega^n = 1$, $\omega \neq 1$) , si nous construisons un logarithme uniforme, nécessairement $\mathrm{Log}\ \omega = 0$, d'où l'intérêt des racines de l'unité :

On sait (voir par exemple : [1], § 5, ex. 33) que l'équation

$$x^{p-1} = 1$$

a $p - 1$ racines 1 , ω , ω^2 , ... , ω^{p-2} dans $\underset{\sim}{Q}_p$, deux à deux incongrues mod p , donc distinctes, et que l'équation

$$x^n = 1$$

à $d = (n , p - 1)$ racines distinctes, qui sont les racines communes à $x^d = 1$ et $x^{p-1} = 1$.

Les seules racines n-ièmes de l'unité sont ses racines $(p - 1)$-ièmes, or elles sont deux à deux incongrues (mod p) et il y en a $p - 1$, donc elles représentent le cercle unité (mod p) , et quel que soit $y \in \underset{\sim}{Q}_p$, $|y| = 1$, il existe un i unique tel que

$$y \equiv \omega^i \pmod{p} \qquad 0 \leqslant i < p - 1 \quad .$$

Soit $y = \omega^i(1 + u)$, $u \in (p)$.

Posons $\operatorname{Log} y = \operatorname{Log}(1 + u)$, ce logarithme vérifie la relation (2), il est continu, et à valeurs dans (p) .

b. Exponentielle multiforme. - Si on cherche à définir une fonction inverse du Log ci-dessus, on est amené à poser, pour $x \in (p)$

$$\exp_i x = \omega^i \exp x = \omega^i E^{x/p} \quad ,$$

ce qui fournit $p - 1$ "déterminations" de l'exponentielle. Chacune de ces déterminations est continue, elles vérifient globalement la relation (1), seule celle que l'on peut appeler principale, $E^{x/p}$, vérifie (1) à elle seule.

Pour prolonger ces nouvelles déterminations hors de (p) , remarquons que $\forall\ \mu \in \underset{\sim}{Z}$, $\mu \geq 1$,

$$\omega^{p^\mu} = \omega^p = \omega \quad .$$

Donc pour $|x| \leq p^{\mu-1}$,

$$\exp_i x = \omega^i\ \varepsilon_\mu^{(p^{\mu-1}x)}$$

prolonge $\exp_i x$.

Il est évident que si on remplace $\mathfrak{k}_\mu$ par l'un de ses $p^\mu - 1$ corps conjugués, nous obtiendrons des déterminations conjuguées de l'exponentielle. Montrons que les $(p - 1)\, p^\mu$ déterminations de $\exp x$, pour $|x| \leq p^{\mu-1}$, sont distinctes (dans la fermeture algébrique Ω de $\underset{\sim}{Q}_p$).

Notons $\exp_i^j x$, $i = 0, 1, \ldots, p - 2$, $j = 1, \ldots, p^\mu$, le j-ième conjugué de $\exp_i x$ $(\varepsilon_\mu = \varepsilon_\mu^1)$. Si $j \neq j'$, $\varepsilon_\mu^j \neq \varepsilon_\mu^{d'}$. Supposons qu'il existe $x \neq 0$ tel que $\exp_i^j x = \exp_i^{j'} x$, $(i , j) \neq (i' , j')$.

Si $j \neq j'$ ces deux nombres sont dans deux extensions conjuguées distinctes de $\underset{\sim}{Q}_p$, donc ne sont égaux que s'ils appartiennent à $\underset{\sim}{Q}_p$, or pour $x \in (p)$, $\exp_i x = \exp_{i'} x \implies \omega^{i-i'} = 1 \implies i = i'$.

Si $j = j' = 1$, par exemple,

$$\exp_i x = \omega_i\ \varepsilon_\mu^{(p^{\mu-1}x)} = \omega_{i'}\ \varepsilon_\mu^{(p^{\mu-1}x)} \implies \omega^{i-i'} = 1 \implies i = i' \quad .$$

Donc il y a exactement $p^{\mu}(p-1)$ déterminations de $\exp x$, à valeurs dans Ω, pour tout $|x| \leqslant p^{\mu-1}$.

c. Logarithme dans $\mathfrak{k}_\mu$. - Si $y \in \mathfrak{k}_\mu$, $y \equiv 1 \pmod{\pi_\mu}$, la série (6) converge pour $u = y - 1$. Soit A_μ l'anneau des entiers de $\mathfrak{k}_\mu$, le corps des restes $\frac{A_\mu}{(\pi_\mu)}$ a p éléments, donc toute unité y de $\mathfrak{k}_\mu$ est dans la classe $\pmod{\pi_\mu}$ d'un ω^i, et comme précédemment, $\operatorname{Log} y = \operatorname{Log} \frac{y}{\omega^i}$, définit le logarithme de toute unité de $\mathfrak{k}_\mu$.

d. Remarque sur les racines p^μ-ièmes des unités de $\mathbb{Q}_p$. - Nous avons démontré au passage, que si $y \in \mathbb{Q}_p$, $|y| = 1$, l'équation $\eta^{p^\mu} = y$ a exactement une racine dans $\mathbb{Q}_p(\varepsilon_\mu)$. Ce résultat algébrique, que nous avons obtenu à l'aide de l'exponentielle, peut aussi se démontrer directement (par des congruences) et on démontre plus précisément que :

Soit $a \in \mathbb{Q}_p$, $a \equiv 1 \pmod{p}$, $a \not\equiv 1 \pmod{p^2}$; soit α une racine de l'équation $\alpha^{p^\mu} = a$, alors $\forall\ x \in \mathbb{Q}_p$, $|x| = 1$, l'équation

$$\xi^{p^\mu} = x$$

a une racine et une seule dans $\mathbb{Q}_p(\alpha)$.

BIBLIOGRAPHIE

[1] BOURBAKI (Nicolas). - Topologie générale, Chapitre 3 : Groupes topologiques. - Paris, Hermann, 1951 (Act. scient. et ind., 916-1143 ; Eléments de Mathématique, 3).

Les résultats classiques sur la convergence des séries exp et Log se trouvent par exemple dans :

CHEVALLEY (Claude). - Sur la théorie du corps de classes dans les corps finis et les corps locaux, J. Fac. Sc. Univ. Tokyo, Section 1, t. 2, 1929-1934, p. 365-476 (Thèse Sc. math. Paris. 1934).

Le reste ne semble pas se rencontrer dans la littérature.