PUBLICATIONS DU DÉPARTEMENT DE MATHÉMATIQUES DE LYON

GÉRARD GOUT

Sur les fonctions exponentielles des corps locaux

Publications du Département de Mathématiques de Lyon, 1970, tome 7, fascicule 3
, p. 105-119

<http://www.numdam.org/item?id=PDML_1970__7_3_105_0>

SUR LES FONCTIONS EXPONENTIELLES DES CORPS LOCAUX

Par Gérard GOUT

Tous les corps locaux (c'est-à-dire les corps localement compacts, non discrets et commutatifs) sont connus : un tel corps est le corps des nombres réels ou celui des nombres complexes, s'il est connexe ; sinon il est une extension de degré fini d'un corps de nombres p-adiques ou bien un corps de séries formelles à coefficients dans un corps fini. (cf. par exemple [1], ouvrage auquel on se réfère pour la terminologie et les notations).

Cette étude a pour objet la description des fonctions exponentielles définies dans un sous-groupe ouvert d'un corps local et de donner la structure (algébrique et topologique) de l'ensemble de ces exponentielles. Enfin, on étudie le problème de leur prolongement, par une voie différente de celle déjà utilisée dans [2]

1. *Définitions et généralités.*

Soit K un corps local. On appelle *fonction exponentielle de* K un homomorphisme continu d'un sous groupe ouvert D du groupe additif K dans le groupe multiplicatif $K^\times$.

D étant fixé, leur ensemble $E(D) = \mathrm{Hom}(D,K^\times)$ est un groupe abélien, pour la loi $(e,f) \mapsto e+f$, où l'on pose $(e+f)(x) = e(x)f(x)$ pour $x \in D$, $f, g \in E(D)$. De plus, si D est muni d'une structure de module sur un anneau A, E(D) est aussi muni d'une structure de A-module, au moyen de $(\alpha,e) \mapsto ae$, où $(\alpha e)(x) = \alpha e(x)$ pour $\alpha \in A$ et $x \in D$ et $e \in E(D)$.

Dans la proposition suivante, on munit E(D) de la *topologie de convergence compacte.*

Proposition 1. - E(D) *est un groupe topologique séparé. De plus, si* D *est un module topologique sur un anneau topologique* A, E(D) *est également un* A*-module topologique.*

Soient C un compact de D et U un ouvert de $K^\times$; on note T(C,U) l'ensemble des $e \in E(D)$ tels que $e(K) \subset U$; lorsque C et U varient T(C,U) décrit un système fondamental de voisinages de o $(x \mapsto 1)$ dans E(D) ; on vérifie immédiatement que E(D) est un groupe topologique séparé.

Sachant que D est un A-module topologique, montrons que E(D) l'est aussi. Soit T(C,U) un voisinage de 0 dans E(D) :

i) $e \in T(aC,U)$ entraine $(ae) \in T(C,U)$, donc $e \mapsto ae$, pour a fixé, est continue en $e = 0$.

ii) il existe un voisinage V de 0 dans D tel que $e(V) \subset U$ puisque e est continue ; l'ensemble des $a \in A$ tels que $aC \subset V$ est un ouvert W de A, contenant 0, (d'après le résultat suivant : soient X, Y, Z des espaces topologiques séparés et $f : X \times Y \to Z$ une application continue ; pour tout compact C et Y et tout ouvert V de Z, l'ensemble des $x \in X$ tels que $f(x,y) \in V$ pour tout $y \in C$ est un ouvert de X) ; ainsi, $a \in W$ entraine $(ae) \in T(C,U)$; ceci montre que pour e fixée, $a \mapsto ae$ est continue en $a = 0$.

iii) soit V' un voisinage ouvert et relativement compact de 0 dans D ; d'après le lemme précédent, il existe un ouvert W', contenant 0, dans A, tel que $W'C \subset V'$; $a \in W'$ et $e \in T(\bar{V}',U)$ entraine $(ae) \in T(C,U)$; donc l'application $(a,e) \mapsto (ae)$ est continue en $(0,0)$.

Ces trois propriétés prouvent que $(a,e) \mapsto (ae)$ est une application continue de $A \times E(D)$ dans $E(D)$.

Remarque : - Par définition de la topologie de la convergence compacte, l'application $(e,x) \mapsto e(x)$ de $E(D) \times D$ dans $K^{\times}$ est continue.

En particulier, pour tout $x \in D$, $e \mapsto e(x)$ est continue sur $E(D)$.

2. *Cas connexe.*

D est nécessairement égal à K, c'est-à-dire à $\mathbb{R}$ (resp. $\mathbb{C}$). $E(\mathbb{R})$ (resp. $E(\mathbb{C})$) est alors un espace vectoriel topologique sur $\mathbb{R}$ (resp. $\mathbb{C}$). Le résultat suivant est bien connu :

Théorème 1. - *Toute fonction exponentielle de* $E(\mathbb{R})$ (resp. $E(\mathbb{C})$) *est de la forme* $x \mapsto a^x$ *où* $a \in \mathbb{R}_+^\times$ (resp. $a \in \mathbb{C}^\times$) *et l'application* $e \mapsto e(1)$ *est un isomorphisme de* $E(\mathbb{R})$ (resp. $E(\mathbb{C})$) *sur* $\mathbb{R}_+^\times$ (resp. $\mathbb{C}^\times$).

3. *Cas discontinu.*

1°) *Supposons d'abord que* K *est un* p*-corps* (p *premier*) *de caractéristique* p.

Théorème 2. - *Pour tout sous-groupe ouvert* D *de* K, E(D) *est réduit à l'exponentielle triviale.*

- En effet, pour $e \in E(D)$ et $x \in D$, on a $px = 0$ et $[e(x)]^p = 1$ en posant $e(x) = 1 + f(x)$, il vient $1 = 1 + [f(x)]^p$ soit $e(x) = 1$.

2°) *Dans toute la suite,* K *désigne un* p*-corps de caractéristique* 0 et on pose $d = [K : \mathbb{Q}_p]$. Soient R le plus grand sous-anneau

compact de K et P l'idéal maximal de R. On sait que $R^\times$ est produit direct de 1+P et du groupe $M^\times$ des racines de l'unité dont l'ordre est étranger à p ; d'autre part, 1+P contient le groupe Γ des racines de l'unité dont l'ordre est une puissance de p.

On a alors les lemmes suivants :

Lemme 1. - *Pour tout couple d'entiers positifs* (m,n), *on a* $(1+P^m)^{p^n} \subset 1+P^{m+n}$ *ceci se démontre facilement par récurrence sur* n.

Lemme 2. - *Pour tout* $e \in E(D)$, *on a* $e(D) \subset 1+P$.

- Si n tend vers l'infini, $p^n x$ tend vers 0 dans D, donc $[e(x)]^{p^n}$ tend vers 1 ; la valuation de K étant discrète ceci entraine $|e(x)|_K = 1$ c'est-à-dire $e(x) \in R^\times$; posons $e(x) = (1+f(x))\times g(x)$ avec $f(x) \in P$ et $g(x) \in M^\times$; le lemme 1 montre que $(1+f(x))^{p^n}$ tend vers 1, donc $[g(x)]^{p^n}$ tend vers 1 dans le groupe discret $M^\times$; ses éléments étant d'ordre étranger à p on a nécessairement $g(x) = 1$; ainsi $e(x) = 1 + f(x) \in 1 + P$.

Lemme 3. - *Toute exponentielle de* E(D) *est égale à* 1 *dans tout sous* $\mathbb{Q}_p$*-espace vectoriel contenu dans* D.

- Soit $x \in D$: pour $n \geqslant 0$ avec $p^{-n}x \in D$ on a $\left[e(p^{-n}x)\right]^{p^n} = e(x)$ donc, d'après le lemme 2, $e(x) \in 1+P^{n+1}$; si x appartient à un sous $\mathbb{Q}_p$-espace vectoriel de D sur lequel e est définie, ceci a lieu pour tout n, donc $e(x) = 1$.

Proposition 2. - *Pour tout* $a \in 1+P$, *il existe un unique homomorphisme continu de* $\mathbb{Z}_p$ *dans* $1+P$ *qui prolonge l'application* $n \mapsto a^n$ *définie dans* $\mathbb{Z}$.

- D'après le lemme 1, l'application $n \mapsto a^n$ est continue sur $\mathbb{Z}$ muni de la topologie p-adique ; $1+P$ étant compact, cet homomorphisme se prolonge de façon unique à $\mathbb{Z}_p$ en un homomorphisme continu

Lemme 4. - *Tout sous-groupe fermé de* K *est un* $\mathbb{Z}_p$*-module topologique.*

- $\mathbb{Z}$ muni de la topologie p-adique opère continûment dans tout sous-groupe D de K par l'application $(n,x) \mapsto nx$: si D est fermé, on peut prolonger cette application en une application continue de $\mathbb{Z}_p \times D$ dans D.

Lemme 5. - *Tout sous-groupe ouvert* D *de* K *est de la forme*

$$D = \sum_{i=1}^{r} \mathbb{Z}_p v_i + \sum_{i=r+1}^{d} \mathbb{Q}_p v_i$$ *où* $(v_i)_{1 \leqslant i \leqslant d}$ *est une base de* K *sur* $\mathbb{Q}_p$ *et* r *le rang du* $\mathbb{Z}_p$*-module* D.

- Soient W le sous $\mathbb{Q}_p$ espace vectoriel maximal contenu dans D et V son supplémentaire dans K ; le $\mathbb{Z}_p$-module $L = (D \cap V) + (R \cap W)$ est ouvert dans K et comme il ne contient pas de sous-espace vectoriel autre que (0), c'est un $\mathbb{Q}_p$ réseau de K [1] ch. II, § 2, prop. 6, cor. 1); d'autre part, D étant dans K, le sous $\mathbb{Q}_p$ espace vectoriel qu'il engendre est égal à K ; le lemme est alors conséquence d'un résultat de [1] : Ch. II, § 2, th. 2, Cor. 1).

D'après la proposition 1, la structure de $\mathbb{Z}_p$ module topologique de D se transmet à E(D). On va comparer cette dernière à celle de 1+P qui, en notation additive, est isomorphe au produit direct $(\mathbb{Z}_p)^d \times \mathbb{Z}_p/p^m \mathbb{Z}_p$ où p^m est l'ordre de Γ ([1], Ch. II, § 3, Prop. 9).

Théorème 3. - *Avec les notations du lemme 5, toute exponentielle de* E(D) *est de la forme*

$$x \mapsto \prod_{i=1}^{r} a_i^{x_i}, \text{ où } a_i \in 1+P \ (1 \leq i \leq r) \text{ et } x = \sum_{i=1}^{d} x_i v_i \in D.$$

E(D) est produit direct de r $\mathbb{Z}_p$*-modules topologiques isomorphes à* 1+P.

- Soit $x \sum_{i=1}^{r} x_i v_i + \sum_{i=r=1}^{d} y_i v_i \in D$; d'après les lemmes 2 et 3 on a $e(v_i) \in 1+P$ pour $i = 1, 2, \ldots, r$ et $e(v_i) = 1$ pour $i = r+1, \ldots, d$; avec la proposition 2, on peut alors écrire $e(x) = \prod_{i=1}^{r} [e(v_i)]^{x_i}$.

Réciproquement, toute famille $(a_i)_{1 \leq i \leq r}$ d'éléments de $1+P$ définit une exponentielle de $E(D)$: $x \mapsto \prod_{i=1}^{r} a_i^{x_i}$. On vérifie aisément que cette application est un isomorphisme de $\mathbb{Z}_p$-module multiplicatif $(1+P)^r$ sur $E(D)$.

En particulier, $E(D)$ est de type fini ; comme $\mathbb{Z}_p$ est compact, $E(D)$ l'est également. D'autre part, d'après la remarque qui suit la proposition 1, l'application $e \mapsto (e(v_i))_{1 \leq i \leq r}$ est continue ; $E(D)$ étant compact c'est un homéomorphisme de $E(D)$ sur $(1+P)^r$.

Proposition 3. - *Pour que* $E(D)$ *contienne des exponentielles injectives, il faut et il suffit que* D *soit un* $\mathbb{Q}_p$*-réseau. Si* e *est une telle exponentielle, la suite exacte* $0 \longrightarrow \mathrm{Im}(e) \longrightarrow 1+P \longrightarrow \Gamma \longrightarrow 0$ *est scindée.*

- La condition est nécessaire d'après le lemme 3. Inversement, soient $D = \sum_{i=1}^{d} \mathbb{Z}_p v_i$ un $\mathbb{Q}_p$-réseau de K et $e(\sum_{i=1}^{d} x_i v_i) = \prod_{i=1}^{d} a_i^{x_i}$ avec $a_i \in 1+P$, une exponentielle de $E(D)$; une telle application est injective si et seulement si la famille $(a_i)_{1 \leq i \leq d}$ est libre dans le $\mathbb{Z}_p$-module $1+P$; celui-ci étant de rang d, de telles familles existent ; alors l'image de e est un $\mathbb{Z}_p$-module libre de rang maximum, c'est donc un facteur direct de $1+P$ dont le quotient est le sous-module de torsion Γ de $1+P$.

4. *Problèmes de prolongement.*

Les hypothèses et notations sont celles de 3, 2°). Le problème se pose de prolonger une fonction de E(D) en une de E(D'), où D' est un sous-groupe de K contenant D. On a le lemme suivant :

Lemme 6. - *Soient* D *et* D' *des sous-groupes ouverts de* K *tels que* $D \subset D'$. *Il existe une base* $(w_i)_{1 \leq i \leq d}$ *de* K *sur* $\mathbb{Q}_p$ *et des entiers positifs* r, r' *et* n_i $(1 \leq i \leq r')$ *tels que*

$$0 \leq r \leq r' \leq d \text{ et que } D = \sum_{i=1}^{r} \mathbb{Z}_p w_i + \sum_{i=r+1}^{d} \mathbb{Q}_p w_i \text{ et}$$

$$D' = \sum_{i=1}^{r'} p^{-n_i} \mathbb{Z}_p w_i + \sum_{i=r'+1}^{d} \mathbb{Q}_p w_i.$$

- Soient w (resp. w') le sous-$\mathbb{Q}_p$-espace vectoriel maximal contenu dans D (resp. D') et V(resp. V') son supplémentaire dans K ; on a déjà vu que $L = (D \cap V) + (R \cap W)$ et $L' = (D' \cap V') + (R \cap W')$ sont des $\mathbb{Q}_p$-réseaux ; $D \subset D'$ entraine $W \subset W'$, donc $W' = W + W_1$ avec $K = W + W_1 + V'$; en décomposant L et L' sur ces sous-espaces (compte tenu de [1], ch. II, § 3, th. 2), on obtient une base $(w_i)_{1 \leq i \leq d}$ de K sur $\mathbb{Q}_p$ telle que

$W = \sum_{i=r+1}^{d} \mathbb{Q}_p w_i$, $W' = \sum_{r'+1}^{d} \mathbb{Q}_p w_i$, $L = \sum_{1}^{d} \mathbb{Z}_p w_i$ et

$L' = \sum_{1}^{d} p^{-n_i} \mathbb{Z}_p w_i$. Comme $D = (D \cap V) + W$ et $D' = (D' \cap V') + W'$, le résultat s'en suit.

Proposition 4. - *Avec les notations du lemme 6, soit* $e \in E(D)$. *Pour que l'on puisse prolonger* e *en une fonction de* $E(D')$ *il faut et il suffit que :*

i) e *soit égale à* 1 *dans la trace sur* D *du plus grand sous* $\mathbb{Q}_p$*-espace vectoriel contenu dans* D'.

ii) pour $1 \leq i \leq r'$, $e(w_i)$ *possède une racine* p^{n_i}*-ème dans* $1+P$.

- Si elle existe, la fonction prolongée est triviale sur W', donc sur $D \cap W'$; d'autre part, pour $x = \sum_{i=1}^{r'} p^{-n_i} x_i w_i \in D' \cap V'$ avec $x_i \in \mathbb{Z}_p$ on doit avoir $e(x) = \prod_{i=1}^{r'} [e(w_i)]^{p^{n_i} x_i}$; ainsi $e(w_i)$ possède une racine p^{n_i}-ème dans $1+P$.

Réciproquement, en prenant une telle racine α_i $(1 \leq i \leq r')$ et en posant $f(x) = \prod_{i=1}^{r'} a_i^{x_i}$ pour $x = \sum_{i=1}^{r'} p^{-n_i} x_i w_i + \sum_{i=r'+1}^{d} y_i w_i \in D'$, on obtient une exponentielle de $E(D')$ qui prolonge e.

Par exemple, on sait que l'exponentielle usuelle de $\mathbb{Q}_p$, somme de la série $\sum_{n \geq 0} \frac{x^n}{n!}$, n'est définie que dans $D = p\,\mathbb{Z}_p$ (si $p \neq 2$) ; soit $D' = \mathbb{Z}_p = p^{-1} D$: (i) est vérifié car $W = W' = (0)$, par contre

(ii) ne l'est pas puisque e(p), qui n'appartient pas à $1+p^2\mathbb{Z}_p$, n'a pas de racine p-ème dans $1+p\mathbb{Z}_p$.

En général, le prolongement d'exponentielles de E(D) à $\mathbb{Q}_p$-réseau contenant D dépend de l'existence de racines p^n-èmes de l'unité dans 1+P (sans restreindre la généralité de cette étude on peut supposer que D est un $\mathbb{Q}_p$-réseau). Pour lever cette difficulté, on peut procéder comme il suit. (comparer avec [2]).

Soit $\bar{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}_p$: d est un corps ultramétrique (non complet) dont la valuation prolonge celle de toute extension K de $\mathbb{Q}_p$ de degré fini. Si l'on identifie K à un sous-corps de $\bar{\mathbb{Q}}_p$, on peut plonger E(D) dans le groupe $\mathrm{Hom}(D, \bar{\mathbb{Q}}_p^{\times})$, muni de la topologie de la convergence compacte. Ceci reste valable pour tout $\mathbb{Q}_p$-réseau $D_n = \bar{p}^n D$ de K (n entier naturel) : la groupe topologique $E(D_n)$ des exponentielles à valeurs dans $\bar{\mathbb{Q}}_p^{\times}$, qui prolongent celles de E(D) à D_n, s'identifie à un sous-groupe de $\mathrm{Hom}(D_n, \bar{\mathbb{Q}}_p^{\times})$ muni de la topologie de la convergence compacte.

La famille des $\mathbb{Q}_p$-réseaux D_n donne naissance à deux systèmes projectifs : (i) celui des $\mathbb{Z}_p$-modules compacts $E(D_n)$ avec des morphismes restrictions évidents.

(ii) celui des groupes séparés $\mathrm{Hom}(D_n, \bar{\mathbb{Q}}_p^{\times})$ avec également des morphismes restrictions.

Ces deux systèmes sont reliés par le morphisme projectif défini par les plongements $\sigma_n : E(D_n) \longrightarrow \mathrm{Hom}\ (D_n, \bar{\mathbb{Q}}_p^\times)$.

L'étude de leur limite fournit la structure de l'ensemble E(D,K) des homomorphismes continus de K dans $\bar{\mathbb{Q}}_p^\times$ qui prolongent les exponentielles de E(D).

Proposition 5. - *Pour tout* $\mathbb{Q}_p$*-réseau* D *de* K, E(D,K) *s'identifie à un sous-groupe compact de* Hom $(K, \bar{\mathbb{Q}}_p^\times)$.

- En utilisant la propriété universelle de la limite projective, on montre que les limites des systèmes (i) et (ii) précédents sont respectivement isomorphes à E(D,K) et Hom $(K, \bar{\mathbb{Q}}_p^\times)$; faisons la démonstration pour (ii) : étant donnés un groupe topologique G et un morphisme projectif constitué des $f_n : G \longrightarrow \mathrm{Hom}\ (D_n, \bar{\mathbb{Q}}_p^\times)$, on peut définir un homomorphisme $g : G \longrightarrow \mathrm{Hom}\ (K, \bar{\mathbb{Q}}_p^\times)$ en associant à $u \in G$ le morphisme $g(u) \in \mathrm{Hom}\ (K, \bar{\mathbb{Q}}_p^\times)$ défini par $g(u)(x) = f_n(u)(x)$ si $x \in D_n$; il est évident que g est l'unique homomorphisme rendant commutatifs les diagrammes voulus. De plus, soit T(C,u) un voisinage de l'élément neutre dans Hom $(K, \bar{\mathbb{Q}}_p^\times)$ où C est un compact de K et U un voisinage de 1 dans $\bar{\mathbb{Q}}_p^\times$; C étant compact, il est contenu dans D_n pour n assez grand, donc pour $h \in \mathrm{Hom}\ (K, \bar{\mathbb{Q}}_p^\times)$ on a $h(C) \subset U$ si et seulement si $(h/D_n)(C) \subset U$.

Comme f_n est continue, il existe un voisinage V de 0 dans G tel

que $f_n(V)(C) \subset U$, ou encore, tel que $g(V) \subset T(C, U)$; g est donc continue.

A la limite, on obtient pour (i) un groupe compact et pour (ii) un groupe séparé. D'autre part, le morphisme projectif des σ_n donne un morphisme injectif de E(D, K) dans Hom $(K, \bar{\mathbb{Q}}_p^\times)$, donc un plongement puisque E(D, K) est compact.

En fait la limite projective de (i) donne $\mathbb{Z}_p$-module compact. Le théorème suivant précise sa structure :

Théorème 4. - *Pour tout* $\mathbb{Q}_p$*- réseau* D *de* K, E(D,K) *est un* $\mathbb{Z}_p$*-module compact isomorphe au produit direct*

$(\mathbb{Z}_p)^{d^2+d} \times (\mathbb{Z}_p/p^m\mathbb{Z}_p)^d$, *où* d *est le degré de* K *sur* $\mathbb{Q}_p$ *et* p^m *l'ordre du groupe* Γ.

- Chaque morphisme restriction $d_n : E(D_n) \to E(D)$ a un noyau isomorphe au produit direct $(\Gamma_n)^d$ où Γ_n désigne le groupe des racines p^n-èmes de l'unité dans $\bar{\mathbb{Q}}_p^\times$, cet isomorphisme étant défini, avec les notations de la proposition 4, par

$$e \in \mathrm{Ker}(d_n) \to (e(\bar{p}^n v_i))_{1 \leq i \leq d} \in (\Gamma_n)^d.$$

On obtient un système projectif de suites exactes dans la catégorie des $\mathbb{Z}_p$-modules compacts :

$$\begin{array}{ccccccc} 0 & \longrightarrow & (\Gamma_{n+1})^d & \longrightarrow & E(D_{n+1}) & \longrightarrow & E(D) \longrightarrow 0 \\ & & \downarrow & & \downarrow d_n & & \downarrow id \\ 0 & \longrightarrow & (\Gamma_n)^d & \longrightarrow & E(D_n) & \longrightarrow & E(D) \longrightarrow 0 \end{array}$$

La première flèche verticale est $x \mapsto x^p$.

A la limite, ce système donne la suite exacte :

$$0 \longrightarrow (\varprojlim \Gamma_n)^d \longrightarrow E(D,K) \longrightarrow E(D) \longrightarrow 0.$$

Soit z_n une racine de l'unité d'ordre p^n telle que $(z_n)^p = z_{n-1}$. Alors l'application $(z_n)^k \in \Gamma_n \longrightarrow k + p^n \mathbb{Z}_p \in \mathbb{Z}_p/p^n \mathbb{Z}_p$ est un isomorphisme des $\mathbb{Z}_p$-modules Γ_n et $\mathbb{Z}_p/p^n \mathbb{Z}_p$. Le système projectif des Γ_n est isomorphe à celui des $\mathbb{Z}_p/p^n \mathbb{Z}_p$ avec les surjections canoniques. On en conclut que $\varprojlim \Gamma_n$ est isomorphe à $\mathbb{Z}_p$.

$E(D)$ et $(\varprojlim \Gamma_n)^d$ étant des $\mathbb{Z}_p$- modules de type fini, $E(D,K)$ en est également un. De plus, le second étant libre, d est un facteur direct de $E(D,K)$: pour le voir on peut appliquer le théorème de structure de [1], ch. II, § 3, th. 2, cor. 2.

Ayant scindée la suite exacte précédente, le résultat s'en suit, connaissant la structure de $E(D)$.

BIBLIOGRAPHIE

[1] A. WEIL, Basic number theory, Berlin (Springer), 1967.

[2] M. C. SARMENT, Prolongement de la fonction exponentielle en dehors de son cercle de convergence.
C. R. Acad. Sc. Paris, 269, 1969, p. 123-125.

Manuscrit remis en Juin 1971

G. GOUT
Ecole supérieure d'ingénieurs de Beyrouth
B. P. 1314
BEYROUTH
(Liban)