Can. J. Math., Vol. XL, No. 4, 1988, pp. 817-832

NOTIONS DE BASE POUR L'ARTHMETIQUE DE $\mathbf{F}_q((1/t))$

YVES HELLEGOUARCH

Le but de ce travail est de définir un certain nombre d'objets de $\mathbf{F}_q((1/t))$ et de fonctions

$$\mathbf{F}_q\left(\left(\frac{1}{t}\right)\right) \to \mathbf{F}_q\left(\left(\frac{1}{t}\right)\right)$$

qui sont analogues à des objets classiques de $\mathbf{R}$ (ou $\mathbf{C}$) et à des fonctions classiques $\mathbf{R} \to \mathbf{R}$ (ou $\mathbf{C} \to \mathbf{C}$) : par exemple $\zeta(1)$, $\zeta(2)$, etc., fractions continues, domaine fondamental du "demi-plan" de Poincaré, séries d'Eisenstein, fonctions multiplement périodiques.

Un tel travail avait été entrepris autrefois par E. Artin [**2**], mais dans un autre esprit, et la fonction zéta que j'ai définie dans [**7**] n'est pas celle d'Artin, mais celle de Carlitz [**3**].

L'intersection de la thèse d'Artin et de ce travail n'est donc pas vide, mais elle n'est pas non plus très étendue bien que je me sois limité aux définitions et aux propriétés les plus élémentaires. En revanche, par son esprit, ce travail se rapproche davantage du point de vue de Carlitz.

Les résultats plus profonds (comme les propriétés de transcendance de $\zeta(h)$) seront démontrés ultérieurement dans des articles plus spécialisés.

1. Notations et definitions. Dans toute la suite q désigne un corps fini à q éléments (dont on suppose la caractéristique $p \neq 2$ lorsque c'est nécessaire).

On écrira aussi $\mathbf{F}_{q^2} = \mathbf{F}_q(i)$, où i^2 est un non-reste de $\mathbf{F}_q$. Si -1 est un non-reste, on choisira de préférence i de telle sorte que $i^2 = -1$.

Par analogie avec la situation classique [**10**] on posera :

$$\begin{cases} Z = \mathbf{F}_q[t], & Q = \mathbf{F}_q(t) \\ R = \mathbf{F}_q\left(\left(\frac{1}{t}\right)\right), & C = \mathbf{F}_{q^2}\left(\left(\frac{1}{t}\right)\right). \end{cases}$$

Si $z \in C$, on a :

Reçu le 21 avril 1987 et en forme revisée le 28 avril 1988.

$$z = a_n t^n + \ldots + a_0 + \frac{a_{-1}}{t} + \ldots + \frac{a_{-n}}{t^n} + \ldots$$

avec $n \in \mathbf{Z}$ et $a_n \neq 0$ si $z \neq 0$.

On pose $|z| = \rho^n$, avec $\rho > 1$, et $\sigma(z) = a_n$. Si $z = 0$, on écrit $|z| = 0$.

Le groupe $GL_2(Z)$ opère sur les droites projectives associées à Q, R et C par transformations homographiques :

$$z \mapsto \frac{az + b}{cz + d}.$$

Un certain nombre de sous-groupes de transformations agissent aussi sur Z, en particulier les translations $\mathscr{T}$:

$$z \mapsto z + \lambda, \quad \lambda \in \mathbf{F}_p$$

et les homothéties $\mathscr{H}$:

$$z \mapsto \lambda z, \quad \lambda \in \mathbf{F}_q^*.$$

2. Sommes de puissances egales. d étant un entier $\geqq 1$, on pose

$$S_q^h(d) = \sum_{\substack{x \in Z \\ |x| \leqq |t|^d}} x^h, \quad Z_q^h(d) = \sum_{\substack{x \in Z, x \neq 0 \\ |x| \leqq |t|^d, \sigma(x) = 1}} x^h.$$

En faisant agir $\mathscr{T}$ et $\mathscr{H}$ sur $\{x \in Z;\ |x| \leqq |t|^d\}$ et $\mathscr{T}$ sur $\{x \in Z;\ x \neq 0,\ \sigma(x) = 1,\ |x| \leqq |t|^d\}$ on a le résultat suivant :

THÉORÈME 1.

(1) $S_q^h(d) = S_q^h(0) Z_q^h(d)$.

(2) *Si h n'est pas un multiple de $q - 1$, $S_q^h(d) = 0$.*

(3) *Si p ne divise aucun des dénominateurs des nombres*

$$\frac{1}{h+1}, \binom{h+1}{1}\frac{B_1}{h+1}, \binom{h+1}{2}\frac{B_2}{h+1}, \ldots, \frac{B_h}{h+1},$$

où les B_i sont les nombres de Bernoulli, alors $Z_q^h(d) = 0$.

Preuve. (1) Posons $E = \{x \in Z;\ |x| \leqq |t|^d\}$.

Par action de $\mathscr{H}$, E se décompose en orbites et dans chaque orbite on peut choisir un polynôme unitaire, donc un ensemble de représentants des orbites est :

$$F = \{x \in Z;\ |x| \leqq |t|^d,\ x \neq 0,\ \sigma(x) = 1\}$$

d'où le résultat.

(2) Si h n'est pas un multiple de $q - 1$ et si ζ est un générateur de $\mathbf{F}_q^*$, on a :

$$S_q^h(0) = \zeta^h + \zeta^{2h} + \ldots + \zeta^{(q-1)h}$$
$$= \zeta' + \zeta'^2 + \ldots + \zeta'^{q-1}$$

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

où $\zeta' = \zeta^h \neq 1$ est une racine de l'unité. Il en résulte que la somme est nulle puisque $\zeta'^{q-1} = 1$.

(3) Par action de $\mathscr{T}$, F se décompose encore en orbites et on peut prendre pour système de représentants des orbites les polynômes dont le terme constant appartient à un système de représentants du groupe quotient $\mathbf{F}_q/\mathbf{F}_p$.

D'après une formule classique [**9**] on a :

$$x^h = \frac{1}{h+1}[B_{h+1}(x+1) - B_{h+1}(x)].$$

Pour chaque orbite, on a :

$$\sum x^h = \frac{1}{h+1}[B_{h+1}(x+p) - B_{h+1}(x)] = 0$$

lorsque les conditions de l'énoncé sont vérifiées, puisque :

$$B_{h+1}(x) = x^{h+1} + \ldots + \binom{h+1}{\nu} B_\nu x^{h+1-\nu} + \ldots + B_{h+1}.$$

Contre-exemples.

$$S_3^2(0) = 1 + 1 = -1, \quad Z_3^2(1) = 0.$$

Remarque. Il est intéressant de comparer (3) avec [**3**] p. 162, Théorème 9.5.

Fonction zéta de Carlitz. On désire développer $1/x^h$, pour $h \geqq 1$, en série en $1/t$. Pour cela on pose :

$$x = a_n t^n + \ldots + a_0 = a_n t^n [1 + t^{-1} R(t^{-1})]$$

avec $R(X) = a_n^{-1}(a_{n-1} + a_{n-2}X + \ldots + a_0 X^{n-1})$. On a alors :

$$\frac{1}{x^h} = a_n^{-h} t^{-nh} \sum_{i=0}^{\infty} \binom{-h}{i} t^{-i} R^i(t^{-1})$$

avec $\binom{-h}{i} \in \mathbf{F}_p$ quel que soit i, donc cette série a un sens.

Définition. Si h est un entier $\geqq 1$, on pose :

$$s(h) = \sum_{\substack{x \in Z \\ x \neq 0}} \frac{1}{x^h}, \quad \zeta(h) = \sum_{\substack{x \in Z \\ x \neq 0 \\ \sigma(x)=1}} \frac{1}{x^h}.$$

Remarque. Il est clair que

$$\zeta(h) = 1 + \frac{a_{-1}}{t} + \frac{a_{-2}}{t^2} + \ldots.$$

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

THÉORÈME 2.
(1) $s(h) = S_q^h(0)\zeta(h)$.
(2) $s(h) = 0$, *dans les conditions du Théorème* 1.
(3) $\prod_{p \in \mathscr{P}} \frac{1}{1 - p^{-h}} = \zeta(h)$

où $\mathscr{P}$ *désigne l'ensemble des polynômes unitaires irréductibles de* Z.

Preuve. (1) Faisons agir $\mathscr{H}$ sur $Z\backslash\{0\}$, un système de représentants des classes d'équivalences est :

$$G = \{x \in Z;\ x \neq 0,\ \sigma(x) = 1\}.$$

Pour la classe de $x \in G$, on a :

$$\Sigma \frac{1}{y^h} = \left(\sum_{\lambda \in \mathbf{F}_q^*} \lambda^{-h}\right) \frac{1}{x^h} = S_q^h(0) \frac{1}{x^h}.$$

(2) Montrons la formule d'Euler.
Soit un entier N quelconque, on a :

$$\prod_{\substack{p \in \mathscr{P} \\ |p| < |t|^N}} \left(1 + \frac{1}{p^h} + \ldots + \frac{1}{p^{(N-1)h}}\right) \equiv \sum_{\substack{x \in Z \\ x \neq 0 \\ \sigma(x) = 1 \\ |x| < |t|^N}} \frac{1}{x^h} \pmod{t^{-N}}.$$

En faisant tendre N vers l'infini, on obtient l'égalité des deux membres.

La démonstration du résultat suivant est assez technique et ne peut trouver place ici. On renvoie à [**3**] et à [**4**] pour deux démonstrations reposant sur des principes différents.

THÉORÈME 3. *Si* $1 \leqq h \leqq q$, *on a* :

$$\zeta(h) = 1 + \sum_{n=1}^{\infty} \frac{(-1)^{nh}}{\prod_{i=1}^{n} (t^{q^i} - t)^h}.$$

COROLLAIRE. $\zeta(1), \ldots, \zeta(q)$ *sont transcendants sur* $\mathbf{Q}$.

Preuve du corollaire. Elle résulte d'une généralisation immédiate d'un résultat de Wade [**11**] : si (λ_n) désigne une suite d'éléments de $\mathbf{F}_q^*$, alors le nombre :

$$\sum_{n=0}^{\infty} \frac{\lambda_n}{\prod_{i=1}^{n} (t^{q^i} - t)^h}$$

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

est transcendant sur Q.

Remarques. (1) Ce corollaire peut être comparé au résultat d'Euler sur les valeurs de $\zeta(2n)$ et à celui de R. Apéry sur l'irrationalité de $\zeta(3)$.

(2) Il entraîne que, pour tout $\nu \in \mathbf{N}$ et $1 \leqq h \leqq q$, $\zeta(hp^{\nu})$ est transcendant sur Q.

3. Description de l'action de $GL_2(\mathbf{Z})$ sur R. Remarquons que l'algorithme des fractions continues correspond à l'action du sous-groupe $G \subset GL_2(Z)$ formé des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ telles que : $ad - bc = \pm 1$.

Si l'on pose

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{et} \quad h_M(z) = \frac{az + b}{cz + d},$$

l'homomorphisme $M \mapsto h_M$ a pour noyau l'ensemble des matrices $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$, avec $\lambda \in \mathbf{F}_q^*$. Il en résulte que si $\det M = \lambda^2$, avec $\lambda \in \mathbf{F}_q^*$, il existe $M' \in SL_2(Z)$ tel que $h_{M'} = h_M$. Donc si -1 n'est pas un carré dans $\mathbf{F}_q$, $GL_2(Z)$ et G ont même action sur R et C.

Le théorème suivant est l'analogue d'un résultat classique ([**6**], p. 142).

THÉORÈME 4. *Pour que z_1 et $z_2 \in R$ aient la même orbite pour l'action de G, il faut et il suffit qu'il existe $\lambda \in \mathbf{F}_q^*$ tel que z_2 et $\pm\lambda^2 z_1$ aient même développement en fraction continue à partir d'un certain rang.*

COROLLAIRE. *Supposons que -1 ne soit pas un reste quadratique dans $\mathbf{F}_q$. Pour que z_1 et z_2 aient la même orbite dans l'action de $GL_2(Z)$ il faut et il suffit qu'il existe $\lambda \in \mathbf{F}_q^*$ tel que z_2 et λz_1 aient même développement en fraction continue à partir d'un certain rang.*

Preuve du Théorème 4. (1) Supposons que z_2 et $\pm\lambda^2 z_1$ aient même développement en fraction continue à partir d'un certain rang :

$$\begin{cases} \pm\lambda^2 z_1 = [a_0, \ldots, a_m, c_1, \ldots] \\ z_2 = [b_0, \ldots, b_n, c_1, \ldots]. \end{cases}$$

On en déduit que si $z' = [c_1, \ldots]$, on a :

$$\begin{cases} \pm\lambda^2 z_1 = \dfrac{p_m z' + p_{m-1}}{q_m z' + q_{m-1}} \\ z_2 = \dfrac{p'_n z' + p'_{n-1}}{q'_n z' + p'_{n-2}} \end{cases}$$

avec deux fractions homographiques provenant de G.

Comme

$$\pm\lambda^2 z_1 = \pm\frac{\lambda z_1 + 0}{0z_1 + \dfrac{1}{\lambda}},$$

on en déduit que z_1 et z_2 ont la même orbite pour G.

(2) Réciproquement, supposons que z_1 et z_2 aient la même orbite pour G, on a :

$$z_2 = \frac{az_1 + b}{cz_1 + d}.$$

(2,1) Développons z_1 en fraction continue :

$$z_1 = [a_0, \ldots, a_{h-1}, z'] = \frac{p_{h-1}z' + p_{h-2}}{q_{h-1}z' + q_{h-2}}.$$

On en déduit que :

$$z_2 = \frac{Az' + B}{Cz' + D}$$

avec

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p_{h-1} & p_{h-2} \\ q_{h-1} & q_{h-2} \end{pmatrix}.$$

Supposons que $z_1 \in R\backslash Q$, alors, lorsque h tend vers l'infini, on a :

$$\begin{cases} |C| = |q_{h-1}|\left|c\dfrac{p_{h-1}}{q_{h-1}} + d\right| \sim |q_{h-1}|\,|cz_1 + d| \\ |D| = |q_{h-2}|\left|c\dfrac{p_{h-2}}{q_{h-2}} + d\right| \sim |q_{h-2}|\,|cz_1 + d|. \end{cases}$$

On en déduit que $|C| > |D|$ lorsque h est assez grand.

(2,2) On utilise ensuite le lemme suivant :

LEMME 1. *Si* $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in G$ *et* $|C| > |D| > 0$, *il existe* $a_0, \ldots, a_m \in Z$ *tels que* $|a_i| > 1$ *pour* $i \geqq 1$ *et* :

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} \lambda p_m & \mu p_{m-1} \\ \lambda q_m & \mu q_{m-1} \end{pmatrix}, \quad \textit{avec } \lambda, \mu \in \mathbf{F}_q^* \textit{ et } \lambda\mu = \pm 1.$$

Preuve. Développons A/C en fraction continue :

$$\frac{A}{C} = [a_0, \ldots, a_m] = \frac{p_m}{q_m}.$$

Puisque $A/C \notin Z$, on a $m \geqq 1$.

On en déduit qu'il existe $\lambda \in \mathbf{F}_q^*$ tel que :

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

$$\begin{cases} A = \lambda p_m \\ C = \lambda q_m. \end{cases}$$

Supposons que

$$\begin{vmatrix} A & B \\ C & D \end{vmatrix} = \begin{vmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{vmatrix},$$

on obtient alors :

$$p_m(q_{m-1} - \lambda D) = q_m(p_{m-1} - \lambda B)$$

donc q_m divise $q_{m-1} - \lambda D$.

Mais on a :

$$|q_{m-1} - \lambda D| \leqq \sup\{ |q_{m-1}|, |D| \} < |q_m|$$

donc $q_{m-1} = \lambda D$ et, par suite, $p_{m-1} = \lambda B$.

Supposons finalement que

$$\begin{vmatrix} A & B \\ C & D \end{vmatrix} = -\begin{vmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{vmatrix},$$

on obtient alors :

$$p_m(q_{m-1} + \lambda D) = q_m(p_{m-1} + \lambda C)$$

et, comme plus haut :

$$q_{m-1} = -\lambda D, \quad p_{m-1} = -\lambda C.$$

Finalement, le théorème de Lagrange se généralise aussi [**2**] :

THÉORÈME 5. *Pour que le groupe d'isotropie de $z \in R$, pour l'action de $GL_2(Z)$ ou de G, ne soit pas trivial, il faut et il suffit que le développement en fraction continue de z soit fini ou périodique.*

4. Description de l'action de $GL_2(Z)$ sur $C \backslash R$. Supposons que l'on ait :

$$z = \frac{az + b}{cz + d}, \quad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(Z)$$

avec z dans une clôture algébrique de $\mathbf{R}$. On en déduit que $z \in Q(\sqrt{\Delta})$ avec :

$$\Delta = (\text{tr } M)^2 - 4 \det M.$$

Il est clair que $\sqrt{\Delta} \in C$, donc que $z \in C$.

Ceci conduit à étendre la classification classique des transformations homographiques de la manière suivante :

$$\begin{cases} M \text{ est parabolique} & \Leftrightarrow (\text{tr } M)^2 = 4 \det M \\ M \text{ est hyperbolique} & \Leftrightarrow |\text{tr } M| > 1 \\ M \text{ est elliptique} & \Leftrightarrow \begin{cases} (\text{tr } M)^2 \neq 4 \det M \\ |\text{tr } M| \leqq 1 \end{cases} \end{cases}.$$

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

Domaine fondamental de **C**. On appellera *domaine fondamental* de C, l'ensemble $\mathscr{D}$ des points $x + iy$ tels que $|x| \leqq 1$, $|y| \geqq 1$ et $\sigma(y) = 1$.

THÉORÈME 6. (1) *L'orbite de tout point de* $C\backslash R$ *pour l'action de* $GL_2(Z)$ *rencontre* $\mathscr{D}$.

(2) *Si* (x, y) *et* (x', y') *sont dans* $\mathscr{D}$ *et si*

$$\begin{cases} |x| < 1, & |x'| < 1 \\ |y| > 1, & |y'| > 1 \end{cases}.$$

Alors (x, y) *et* (x', y') *ne peuvent avoir la même orbite que s'ils sont égaux.*

Preuve du Théorème 6. (1) Soit $z_0 = x_0 + iy_0$, $x_0, y_0 \in \mathbf{R}$, $y_0 \neq 0$ et soit $[x_0]$ la partie entière de x_0, c'est-à-dire l'élément $a \in Z$ tel que $|x_0 - a| < 1$, on pose :

$$z_0' = z_0 - [x_0] = x_0' + iy_0'.$$

Si $|y_0'| > 1$, on remplace z_0' par $[\sigma/y_0']^{-1} z_0' \in \mathscr{D}$.

Sinon, on pose :

$$z_1 = -\frac{1}{z_0'} = x_1 + iy_1$$

et on a :

$$|y_1| > |y_0'|.$$

Donc

$$z_1' = z_1 - [x_1] = x_1' + iy_1'$$

est tel que $|x_1'| < 1$ et $|y_1'| > |y_0'|$.

En remplaçant z_1' par $[\sigma(y_1')]^{-1} z_1'$ on obtient un point de $\mathscr{D}$ lorsque $|y_1'| > 1$.

(2) Supposons que

$$z' = \frac{az + b}{cz + d},$$

avec

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(Z),$$

et $z' \neq z$. Nous avons :

$$\left|\frac{y}{y'}\right| = |c^2 z\bar{z} + 2cdx + d^2|$$

avec $\bar{z} = x - iy$.

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

Si $c = 0$, alors $ad \in \mathbf{F}_q^*$, donc $a = \lambda \in \mathbf{F}_q^*$ et $d = \mu \in \mathbf{F}_q^*$

$$z' = \frac{\lambda}{\mu} z + b', \quad \text{avec } b' \in Z \quad \text{et}$$

$$|b'| \leqq \sup\left\{ |x'|, \left|\frac{\lambda}{\mu} x\right| \right\} < 1$$

donc $b' = 0$.

Il reste $y' = (\lambda/\mu)y$, d' où $\lambda/\mu = 1$ puisque y et y' sont unitaires, donc $z' = z$ ce qui est contraire à l'hypothèse.

Si $|d| > |c| > 0$, alors :

$$\left|\frac{y}{y'}\right| = |c^2 z\bar{z} + d^2|.$$

Il ne peut pas y avoir de simplification du terme de plus haut degré en t dans $c^2 z\bar{z} + d^2$, sinon i^2 serait un carré dans $\mathbf{F}_q^*$, donc

$$\left|\frac{y}{y'}\right| > 1.$$

Si $|d| \leqq |c|$, on a encore :

$$\left|\frac{y}{y'}\right| = |c^2 z\bar{z}| > 1.$$

Donc $|y| > |y'|$ et on obtient une contradiction en inversant M.

Remarque. Pour l'étude de la frontière de $\mathscr{D}$, voir [**8**].

4. Series d'Eisenstein. Comme dans [**1**] nous désignons par $\tilde{C}$ le complété d'une clôture algébrique de $R = \mathbf{F}_q((1/t))$.

Soit M l'ensemble des Z-modules discrets et de type fini de $\tilde{C}$ et soit X_M l'espace vectoriel sur $\mathbf{F}_p$ de base M.

Lorsqu'on se donne deux Z-modules Γ et Γ' de M tels que $\Gamma' \subset \Gamma$, on sait que Γ possède une base $(e_1, \ldots, e_r)$ telle que :

$$\Gamma' = Za_1 e_1 + \ldots + Za_r e_r$$

avec $a_i \in Z$ pour $i = 1, \ldots, r$.

Définition. Lorsque $a_1 \ldots a_r \neq 0$, on pose :

$$[\Gamma : \Gamma'] = \frac{a_1 \ldots a_r}{\sigma(a_1 \ldots a_r)}.$$

Lorsque $a_1 \ldots a_r = 0$, on pose :

$$[\Gamma : \Gamma'] = \infty.$$

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

Comme dans [**10**], nous définissons, pour tout $n \in Z$, unitaire, un *opérateur de Hecke* $T(n)$ par son action sur la base M de X_M :

$$T(n)(\Gamma) = \sum_{\substack{\Gamma' \subset \Gamma \\ [\Gamma:\Gamma']=n}} \Gamma'.$$

Il en résulte que pour tout $\xi \in X_M$, on a :

$$T(n)(\xi) = \sum_{\Lambda \in M} \nu_\Lambda(\xi)\Lambda, \quad \text{avec } \nu_\eta(\xi) \in \mathbf{F}_p.$$

Lorsque F est une application : $M \to \tilde{C}$, on définit $T(n)F$ par :

$$[T(n)F](\Gamma) = \sum_{\Lambda \in M} \nu_\Lambda(\Gamma)F(\Lambda).$$

PROPOSITION. (1) *Si* $(m, n) = 1$, *on a* : $T(m)T(n) = T(mn)$.
(2) *Si* l *est irréductible, on a* : $T(l^h) = T(l)^h$.

Preuve. Cette proposition se démontre comme la Proposition 10, p. 160 de [**10**].

COROLLAIRE. *L'algèbre* H *engendré par les* $T(l)$ *sur* $\mathbf{F}_p$ *est celle des polynômes à une infinité dénombrable d'indéterminées.*

Définition. Pour tout entier $n > 0$ et tout $\Gamma \in M$, on définit la *série d'Eisenstein* $e_n(\Gamma)$ par :

$$e_n(\Gamma) := \sum_{\substack{\gamma \in \Gamma \\ \gamma \neq 0}} \frac{1}{\gamma^n}.$$

Cette définition a un sens en vertu du lemme suivant.

LEMME 2. *Pour tout* $x \in \tilde{C}$, $|x + \gamma|$ *tend vers l'infini lorsque* γ *tend vers l'infini dans* Γ *suivant le filtre des complémentaires des parties finies.*

THÉORÈME 7. *Les applications* e_n *sont invariantes par les opérateurs de Hecke.*

Preuve. On reprend la démonstration de la Proposition 13 de [**10**], p. 168. Il s'agit de montrer que si l est un polynôme irréductible unitaire de Z, on a :

$$T(l)e_n(\Gamma) = e_n(\Gamma).$$

Comme dans [**10**], on écrit :

$$T(l)e_n(\Gamma) = \sum_{\substack{\Gamma' \subset \Gamma \\ [\Gamma:\Gamma']=l}} \sum_{\gamma \in \Gamma'}{}' \frac{1}{\gamma^n}.$$

Désignons par r le rang de Γ.

Si $\gamma \in l\Gamma$, il y a exactement $(|l|^r - 1)/(|l| - 1)$ sous-réseaux Γ' de Γ contenant γ et tels que $[\Gamma:\Gamma'] = l$: ils sont en correspondance bijective avec les hyperplans de l'espace vectoriel $\Gamma/_{l\Gamma}$. Comme :

$$\frac{|l|^r - 1}{|l| - 1} = |l|^{r-1} + \ldots + 1 = 1 \text{ dans } \mathbf{F}_p$$

tout se passe comme si γ n'appartenait qu'à un seul sous-réseau Γ'.

Si $\gamma \in \Gamma \backslash l\Gamma$, il y a exactement $(|l|^{r-1} - 1)/(|l| - 1)$ sous-réseaux Γ' de Γ contenant γ et tels que $[\Gamma:\Gamma'] = l$: on le voit de la même façon et on obtient la même conclusion.

Remarques. (1) Si n n'est pas un multiple de $q - 1$, $e_n(\Gamma) = 0$. Pour voir cela on fait agir les homothéties de $\mathscr{H}$ sur Γ et on désigne par $\mathscr{S}$ un système de représentants des orbites de $\Gamma \backslash \{0\}$, on a alors :

$$e_n(\Gamma) = S_q^n(0) \sum_{\gamma \in \mathscr{S}} \frac{1}{\gamma^n}$$

d'où le résultat d'après le Théorème 1 (deuxième partie).

(2) D'autre part, si n est un multiple de $q - 1$, on a :

$$\operatorname*{Lim}_{|\tau| \to \infty} e_n(Z + Z\tau) = -\zeta(n) \neq 0.$$

En effet si $|\tau| > |t|^N$, on a :

$$e_n(Z + Z\tau) \equiv -\sum_{\substack{x \in Z \backslash \{0\} \\ \sigma(x) = 1}} \frac{1}{x^n}, \text{ modulo } t^{-nN}$$

d'où le résultat en faisant tendre N vers ∞.

(3) L'hypothèse "Γ est un $\mathbf{F}_{q^2}$-espace vectoriel" doit être ajoutée dans l'énoncé du Théorème 6 de [7].

5. Exemples de fonctions multiplement periodiques. Dans ce paragraphe, Γ désigne un Z-module discret de type fini de $\tilde{C}$ et on pose toujours $\Gamma' = \Gamma \backslash \{0\}$.

Définition. Pour tout entier $n > 0$, on pose (comme dans le paragraphe 4) :

$$e_n(\Gamma) := \sum_{\gamma \in \Gamma'} \frac{1}{\gamma^n}$$

et si $x \in \tilde{C} \backslash \Gamma$:

$$(1) \qquad E_n(x, \Gamma) := \sum_{\gamma \in \Gamma} \frac{1}{(x + \gamma)^n} = \frac{1}{x^n} + \sum_{\gamma \in \Gamma'} \frac{1}{(x + \gamma)^n}.$$

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

Il est clair que tout élément de Γ est une période de $E_n(x, \Gamma)$ et que E_n est continue sur $\tilde{C}\backslash\Gamma$ et indéfiniment dérivable.

Remarque. Lorsque $|x| < \inf\{|\gamma|;\ \gamma \in \Gamma'\}$ on peut donner le développement de $E_n(x, \Gamma)$ en série de puissances de x^n de la manière suivante. On développe chaque terme de la somme par la formule du binôme :

$$(x + \gamma)^{-n} = \gamma^{-n}\left(1 + \frac{x}{\gamma}\right)^{-n} = \sum_{h=0}^{\infty}\binom{-n}{h}\frac{x^h}{\gamma^{h+n}}$$

et on regroupe les coefficients de x^h :

$$(2)\qquad E_n(x, \Gamma) = \frac{1}{x^n} + \sum_{h=0}^{\infty}\binom{-n}{h}e_{h+n}(\Gamma)x^h$$

$$= \frac{1}{x^n} + (-1)^n \sum_{m \geqq n}\binom{m-1}{n-1}e_m(\Gamma)x^{m-n}$$

en tenant compte du fait que $e_m(\Gamma) = 0$ lorsque m est impair.

Exemple. Si $\Gamma = Z$ et $n = 1$, on a :

$$E_1(x, Z) = \frac{1}{x} + \sum_{l \geqq 1}\zeta(l(q-1))x^{l(q-1)-1}.$$

En effet, il est clair que :

$$e_m(Z) = S_q^m(0)\zeta(m)$$

où l'on pose :

$$S_q^m(0) = \sum_{\lambda \in \mathbf{F}_q^*}\lambda^m.$$

Maintenant on sait que $S_q^m(0) = 0$ si $q - 1$ ne divise pas m et que $S_q^m(0) \equiv -1$ si $q - 1$ divise m.

Formules d'addition. (a) Nous allons utiliser la méthode d'Eisenstein [**12**] pour obtenir une formule d'addition pour E_1.

Cette méthode est basée sur l'identité :

$$(3)\qquad \frac{1}{pq} = \frac{1}{pr} + \frac{1}{qr} \quad \text{si } r = p + q.$$

Prenons :

$$p = x + \gamma,\quad q = y + \gamma' - \gamma,\quad z = x + y,\quad r = z + \gamma'$$

et sommons d'abord par rapport à γ dans (3) on trouve :

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

$$(4)\qquad \sum_{\gamma} \frac{1}{x+\gamma}\frac{1}{y+\gamma'-\gamma} = \frac{1}{x+y+\gamma'}[E_1(x)+E_1(y)]$$

car $E_1(y+\gamma') = E_1(\gamma)$.

Sommons par rapport à γ' dans (4) on a :

$$E_1(x)E_1(y) = E_1(x+y)[E_1(x)+E_1(y)]$$

où :

$$(5)\qquad \frac{1}{E_1(x+y)} = \frac{1}{E_1(x)} + \frac{1}{E_1(y)}.$$

Remarques. (1) Cette relation est à comparer à la formule classique :

$$\frac{1}{E_1(x+y)} = \frac{E_1(x)+E_1(y)}{E_1(x)E_1(y)-\pi^2}$$

et tout se passe ici comme si $\pi^2 = 0$ (voir [**12**], page 12) contrairement à ce qui se passait pour les valeurs de $\zeta(n)$ (voir [**11**]).

(2) Supposons que $E_1(x) \neq 0$, alors d'après (5) :

$$x+y \in \Gamma \Leftrightarrow E_1(x)+E_1(y) = 0.$$

(b) Nous allons maintenant chercher une formule d'addition pour E_n.

Dérivons (formellement) $(m-1)$ fois l'identité (3) par rapport à p, nous avons (en caractéristique nulle) :

$$(6)\qquad \frac{1}{p^m q} = \sum_{h=0}^{m-1} \frac{1}{p^{m-h}r^{h+1}} + \frac{1}{qr^m}.$$

Dérivons $(n-1)$ fois l'identité (6) par rapport à q, nous avons (en caractéristique nulle) :

$$(7)\qquad \frac{1}{p^m q^n} = \sum_{h=0}^{m-1} \binom{n+h-1}{h} \frac{1}{p^{m-h}r^{h+n}} + \sum_{k=0}^{n-1} \binom{m+k-1}{k} \frac{1}{q^{n-k}r^{m+k}}.$$

Maintenant nous remarquons que ces identités sont à coefficients entiers donc subsistent en caractéristique p.

Isolons les termes correspondant à $h = m-1$ et $k = n-1$ et résolvons (7) en $E_{m+n-1}(x+y)$ nous avons :

$$\binom{m+n-2}{m-1}[E_1(x)+E_1(y)]E_{m+n-1}(x+y)$$
$$= E_m(x)E_n(y) + P[E_i(x), E_j(y), E_k(x+y)]$$

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

où P désigne un polynôme à coefficients entiers et où $i \in \{2, \ldots, m\}$, $j \in \{2, \ldots, n\}$, $k \in \{\inf(m, n), ., m + n - 2\}$.

Prenons $m = 1$, on trouve :

$$[E_1(x) + E_1(y)]E_n(x + y)$$

$$= E_1(x)E_n(y) - \sum_{j=2}^{n} E_j(y)E_{n+1-j}(x + y).$$

Cette formule permet de déduire, par récurrence sur n, le résultat suivant :

LEMME 3. *Pour tout $n \geqq 1$, $E_n(x + y)$ est une fonction rationnelle des $E_i(x)$ et des $E_j(y)$ dont le dénominateur peut être pris égal à $[E_1(x) + E_1(y)]^n$.*

Relations algébriques entre les E_n. On pose dans la formule (7)

$$p = x + \gamma, \quad q = -x - \gamma + \gamma', \quad r = \gamma'$$

et on fait la somme (successivement) par rapport à γ et γ', on trouve :

$$(8) \quad (-1)^n(E_mE_n - E_{m+n}) = \sum_{h=0}^{m-1} \binom{n + 1 - 1}{h} E_{m-h}e_{n+h} + \sum_{k=0}^{n-1} (-1)^{n-k}\binom{m + k - 1}{k} E_{n-k}e_{m+k}$$

et en particulier, pour $m = 1$, on trouve :

$$(9) \quad E_1E_n - E_{n+1} = \sum_{k=0}^{n-2} (-1)^k E_{n-k}e_{k+1}.$$

THÉORÈME 8. (1) *E_n est un polynôme en E_1 dont les coefficients appartiennent à*

$$\mathbf{F}_p[e_1, e_2 \ldots] := \mathbf{F}_p[e(\Gamma)].$$

(2) *Si $n < q$, on a $E_n = E_1^n$.*

(3) *Si $n = q + 1$, on a $E_n = E_1^n - e_{q-1}E_1^2$.*

Preuve. (1) La première assertion se démontre par récurrence sur n.

(2) La seconde assertion résulte de (9) (par exemple) et de la remarque suivante :

$$e_h(\Gamma) = S_q^h(0) \sum_{\gamma \in \mathcal{S}} \frac{1}{\gamma^h}$$

où $\mathcal{S}$ est un système de représentants des orbites de $\Gamma' = \Gamma \backslash \{0\}$ pour l'action de $\mathbf{F}_q^*$.

https://doi.org/10.4153/CJM-1988-036-0 Published online by Cambridge University Press

Comme $S_q^h(0) = 0$ si $q - 1$ ne divise pas h, on a $e_h(\Gamma) = 0$ si $h < q - 1$, d'où (d'après 9) :

$$E_1E_n = E_{n+1} \quad \text{si } n - 1 < q - 1.$$

(3) Supposons maintenant que $n = q$, alors la formule (9) donne le résultat :

$$\begin{aligned} E_1E_n - E_{n+1} &= -E_2e_{q-1} \\ &= -E_1^2e_{q-1}. \end{aligned}$$

THÉORÈME 9. *Pour tout* $n \geqq 1$, $E_n(x + y)$ *est une fonction rationnelle de* $E_1(x)$ *et de* $E_1(y)$ *dont le dénominateur peut être pris égal à* $[E_1(x) + E_1(y)]^n$ *et dont les coefficients sont dans* $\mathbf{F}_p(e(\Gamma))$.

Preuve. Résulte de Lemme 4 et du Théorème 8.

Formules de multiplication. On se propose de démontrer le théorème suivant.

THÉORÈME 10. *Pour tout* $n \geqq 1$ *et pour* $\lambda \in Z$, *la fonction* $E_n(\lambda x)$ *est une fonction rationnelle de* $E_1(x)$ *à coefficients dans* $\tilde{C}$ (*et même dans un sous-corps de* $\tilde{C}$ *que l'on peut préciser*).

Preuve. On pose $\Gamma_\lambda = \{\lambda\gamma;\ \gamma \in \Gamma\}$. Γ_λ est un sous-module de Γ d'indice fini. Soit $\mathscr{R}$ un système de représentants des éléments de Γ modulo Γ_λ, choisi de telle sorte que $0 \in \mathscr{R}$.

Il est clair que :

$$(10) \quad E_n(x, \Gamma) = \sum_{r \in \mathscr{R}} E_n(x + r, \Gamma_\lambda).$$

Compte-tenu de l'homogénéité de la formule (10) on a :

$$\lambda^n E_n(x, \Gamma) = \sum_{r \in \mathscr{R}} E_n\left(\frac{x + r}{\lambda}, \Gamma\right)$$

et en remplaçant x par λx, on trouve :

$$(11) \quad \lambda^n E_n(\lambda x) = \sum_{r \in \mathscr{R}} E_n\left(x + \frac{r}{\lambda}\right).$$

Les formules d'addition (Théorème 9) entraînent le résultat.

Remarques. (1) Le corps auquel on fait allusion dans l'énoncé, s'obtient en adjoignant $E_1(r/\lambda)$, $r \in \mathscr{R}$, à $\mathbf{F}_p(e(\Gamma))$.

(2) On voit donc que $E_n(\lambda x + \mu y)$ s'exprime par des formules rationnelles en $E_1(x)$ et $E_1(y)$ pour chaque valeur de $(\lambda, \mu) \in Z^2$.

(3) Lorsque $\Gamma = Z\alpha$, où α désigne l'un des zéros de la fonction ψ de Carlitz tels que :

$$|\alpha| = \rho^{q/(q-1)}$$

un résultat de Schöbe ([5], p. 1.45) montre que

$$E_1(x)\psi(x) = 1.$$

Le Théorème 10 est donc une généralisation de la relation ([5], p. 1.27) :

$$\psi(\lambda x) = \sum_{j=0}^{\deg(\lambda)} (-1)^j \frac{\psi_j(\lambda)}{F_j} \psi^{q^j}(x).$$

BIBLIOGRAPHIE

1. E. Artin, *Algebraic number and algebraic functions* (Gordon and Breach, 1967).
2. ——— *Quadratische Körpern im Gebiete der köheren Kongruenzen* in *The collected papers of Emil Artin* (Addison-Wesley, 1965).
3. L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. *1* (1935), 137-168.
4. G. Damamme, *Irrationalité de $\zeta(s)$ dans le corps des séries formelles* $\mathbf{F}_q((1/t))$, C.R. Math. Ac. Sci. Canada *9* (1987), 207-212.
5. J. M. Geijsel, *Transcendence in fields of positive characteristic*, Thèse (1978), Amsterdam.
6. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers* (Oxford, 1954).
7. Y. Hellegouarch, *Propriétés arithmétiques des séries formelles à coefficients dans un corps fini*, C.R. Math. Acad. Sci. Canada *8* (1986), 115-120.
8. S. Ouro-Sama, *Algèbre géométrique d'une extension quadratique avec référence spéciale aux corps de séries formelles*, Thèse de 3ème cycle, Université de Caen (1987).
9. H. Rademacher, *Topics in analytic number theory* (Springer, 1973).
10. J. P. Serre, *Cours d'arithmétique* (P.U.F., 1970).
11. L. I. Wade, *Certain quantities transcendental over $GF(p^n, x)$, II*, Duke Math. J. *10* (1943), 587-594.
12. A. Weil, *Elliptic functions according to Eisenstein and Kronecker* (Springer, 1976).

Université de Caen,
Caen Cedex, France