SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Rationalité des fonctions ζ des variétés algébriques

Séminaire N. Bourbaki, 1960, exp. n° 198, p. 415-425

<http://www.numdam.org/item?id=SB_1958-1960__5__415_0>

Séminaire BOURBAKI
12e année, 1959/60, n° 198

Février 1960

RATIONALITÉ DES FONCTIONS ζ DES VARIÉTÉS ALGÉBRIQUES

par Jean-Pierre SERRE

(d'après Bernard DWORK [4])

1. Introduction.

La fonction ζ d'un schéma S de type fini sur $\underset{\sim}{Z}$ est définie par le produit eulérien :

$$\zeta_S(s) = \prod_P \frac{1}{(1 - 1/N(P)^s)} \quad , \tag{1}$$

où P parcourt l'ensemble des points fermés de S, et où $N(P)$ est le nombre d'éléments du corps des restes $\varkappa(P)$ correspondant. Ce produit converge pour $R(s)$ assez grand, et on conjecture qu'il se prolonge en une fonction méromorphe dans tout le plan complexe.

Considérons en particulier, un schéma V de type fini sur $\underset{\sim}{F}_q$, corps fini à q éléments (c'est ce que certains appellent une "variété algébrique définie sur $\underset{\sim}{F}_q$"). On a alors $\underset{\sim}{F}_q \subset \varkappa(P)$, et si $\deg(P)$ désigne le degré de cette extension, on a :

$$N(P) = q^{\deg(P)} \quad , \tag{2}$$

ce qui conduit à changer de variable, et à poser $t = q^{-s}$. On obtient ainsi la fonction :

$$Z_V(t) = \prod_P \frac{1}{1 - t^{\deg(P)}} \quad , \tag{3}$$

qui est une série entière en t, à coefficients dans $\underset{\sim}{Z}$.

Notons N_s le nombre de points du $\underset{\sim}{F}_q$-schéma V à valeurs dans l'extension $\underset{\sim}{F}_{q^s}$ de $\underset{\sim}{F}_q$. Un calcul simple donne :

$$Z_V(t) = \exp\left\{\sum_{s=1}^{\infty} N_s \, t^s/s\right\} \quad . \tag{4}$$

WEIL, à qui ces définitions sont dues, avait conjecturé que Z_V est une fonction rationnelle de t, et l'avait vérifié dans certains cas (cf. [5] ainsi que l'exposé de DELSARTE [2]). DWORK vient de résoudre la question :

THÉORÈME ([4]). - Pour tout schéma V de type fini sur le corps $\underset{\sim}{F}_q$, la fonction $Z_V(t)$ est une fonction rationnelle.

On peut se borner au cas où q est un nombre premier p, puisque $\underset{\sim}{F}_q$ est de type fini sur $\underset{\sim}{F}_p$. De plus, si V' et V'' sont des sous-schémas de V, avec $V' \cup V'' = V$ et $V' \cap V'' = W$, on a :

$$Z_V = Z_{V'} \cdot Z_{V''} \cdot Z_W^{-1} \qquad (5)$$

Cette formule permet, par un argument combinatoire facile, de ramener le théorème au cas où V est affine, et même au cas où V est défini par une seule équation

$$f(X_1, \ldots, X_n) = 0 \text{ , à coefficients dans } \underset{\sim}{F}_p \qquad (6)$$

Dans ce cas, N_s est simplement le nombre de solutions de l'équation (6) dans le corps à p^s éléments.

2. Un critère de rationalité.

On va d'abord rappeler un critère classique :

Soit k un corps, et soit

$$F(t) = \sum_{s=0}^{\infty} A_s t^s , \qquad A_s \in k \qquad (7)$$

une série formelle. Si s et m sont deux entiers $\geqslant 0$, posons

$$N_{s,m} = \det(A_{s+i+j}) , \qquad 0 \leqslant i \leqslant m , \qquad 0 \leqslant j \leqslant m \qquad (8)$$

PROPOSITION 1. - Pour que F soit quotient de deux polynômes en t à coefficients dans k (i. e. pour que F soit rationnelle), il faut et il suffit qu'il existe un entier $m \geqslant 0$ tel que $N_{s,m} = 0$ pour tout s assez grand.

Pour la démonstration, voir [1], ainsi que BOURBAKI, Algèbre IV, paragraphe 5, exercice 3

Supposons maintenant que les A_s soient entiers. On pourra donc parler à la fois de leur valeur absolue usuelle (induite par le plongement dans $\underset{\sim}{C}$), notée $|A|$, et de leur valeur absolue p-adique, notée $|A|_p$, comme d'habitude, on suppose cette dernière normée par la formule du produit, i. e. $|p^a|_p = p^{-a}$. De plus, on se donne un corps valué complet Ω, algébriquement clos, contenant $\underset{\sim}{Q}_p$, et dont la valeur absolue prolonge celle de $\underset{\sim}{Q}_p$. Une série

$$f = \sum_{i=0}^{\infty} a_i t^i , \qquad a_i \in \Omega ,$$

sera dite holomorphe dans le disque $|t|_p < r$ si elle converge absolument dans ce disque ; un quotient de deux telles séries sera appelé une fonction méromorphe. Si f est holomorphe pour $|t|_p < r$, et si $r' < r$, on démontre qu'on peut écrire f sous la forme $P.f'$, où P est un polynôme, et où f' est une série holomorphe ainsi que son inverse dans le disque $|t|_p < r'$ (on ne peut plus, ici, se servir de l'intégrale de Cauchy, il faut raisonner directement, en se servant du "polygone de Newton" de f, ce n'est pas très difficile).

PROPOSITION 2. - *Soit* $F = \sum_{s=0}^{\infty} A_s t^s$ *une série à coefficients entiers, et soit* p *un nombre premier. Supposons qu'il existe deux nombres réels positifs* R *et* r, *avec* $Rr > 1$, *tels que* F *soit méromorphe dans le disque* $|z| < R$ *de* $\mathbb{C}$ *ainsi que dans le disque* $|z|_p < r$ *de* Ω. *Alors* F *est rationnelle.*

Lorsque $R > 1$, on retrouve un résultat d'Emile BOREL [1]. Supposons donc $R < 1$, d'où $r > 1$. Par hypothèse, il existe des séries entières :

$$A(t) = \sum_{i=0}^{\infty} a_i t^i, \qquad B(t) = \sum_{i=0}^{\infty} B_i t^i, \qquad a_i, B_i \in \Omega \qquad (9)$$

holomorphes dans $|z|_p < r$, et telles que $B = A.F$. D'après ce qui a été dit ci-dessus, on peut même supposer que A est un polynôme (quitte à diminuer un peu r), et aussi que $a_o = 1$. Quitte à diminuer encore un peu r, on a des inégalités :

$$|B_s|_p \leq r^{-s} \quad \text{pour } s \text{ assez grand}, \qquad (10)$$

$$|A_s| \leq R^{-s} \quad \text{pour } s \text{ assez grand}. \qquad (11)$$

Soit e le degré de A, et choisissons un entier m tel que $R^{m+1} r^{m+1-e} = k$ soit > 1, ce qui est possible puisque $Rr > 1$. On va appliquer le critère de la proposition 1.

Puisque $B = A.F$, on a :

$$B_{s+e} = A_{s+e} + a_1 A_{s+e-1} + \ldots + a_e A_s \qquad (12)$$

Dans le déterminant $N_{s,m} = \det(A_{s+i+j})$, $0 \leq i, j \leq m$, on peut donc remplacer les A_{s+i+j}, $j \geq e$, par les B_{s+i+j}. En appliquant (10), et en tenant compte du fait que $|A_s|_p \leq 1$, on en déduit :

$$|N_{s,m}|_p \leq r^{-(m+1-e)s}, \quad \text{pour } s \text{ assez grand}. \qquad (13)$$

D'autre part, on tire de (11) l'inégalité :

(14) $$|N_{s,m}| \leq R^{-(m+1)(s+2m)} , \qquad \text{pour } s \text{ assez grand} .$$

D'où :

(15) $$|N_{s,m}| . |N_{s,m}|_p \leq k_1 . k^{-s} , \qquad k_1 \text{ indépendant de } s .$$

Comme $k > 1$, ceci entraîne $|N_{s,m}| . |N_{s,m}|_p < 1$ pour s assez grand, et comme $N_{s,m}$ est un entier, ceci entraîne $N_{s,m} = 0$,

C. Q. F. D.

REMARQUE. - On trouvera dans [4] un énoncé généralisant la proposition 2 au cas où l'on prend les A_i dans un corps de nombres K , et où l'on fait des hypothèses de méromorphie pour un nombre fini de "places" de K .

Application à la fonction $Z_V(t)$. - Si V est plongé dans l'espace affine à n dimensions, la série $Z_V(t)$ admet comme majorante la série $1/(1 - p^n t)$, ce qui montre qu'elle est holomorphe dans le disque de rayon p^{-n} . Pour pouvoir lui appliquer la proposition 2, il faut donc montrer qu'elle est méromorphe (au sens p-adique) dans un disque de rayon $> p^n$. En fait, on verra que $Z_V(t)$ est même méromorphe dans tout Ω , autrement dit est quotient de deux séries entières à coefficients dans Ω , ayant chacune un rayon de convergence infini ; ces séries entières seront construites explicitement, à partir de l'équation f définissant le schéma V . Ceci sera fait au paragraphe 5 ; les paragraphes 3 et 4 sont consacrés à des constructions préliminaires.

3. Factorisation des caractères additifs des corps finis.

On note K le corps des restes de Ω ; c'est un corps algébriquement clos de caractéristique p ; il contient donc tous les $\mathbb{F}_{p^s}$. Tout élément de K a un unique "représentant multiplicatif" dans Ω . Les représentants multiplicatifs des éléments de $\mathbb{F}_{p^s}$ sont les racines $(p^s - 1)$-ièmes de l'unité et 0 . On note Λ l'anneau des entiers de Ω ; on a $\Lambda \cap \mathbb{Q}_p = \mathbb{Z}_p$, anneau des entiers p-adiques. Enfin, on pose

$$|x|_p = p^{-\mathrm{ord}(x)} , \qquad x \in \Omega .$$

On a $\mathrm{ord}(p) = 1$.

Soient t et Y deux indéterminées. Considérons la série formelle

(16) $$H(t , Y) = (1 + Y)^t = \sum_{m=0}^{\infty} \binom{t}{m} . Y^m , \quad \text{où} \quad \binom{t}{m} = \frac{t(t - 1) \ldots (t - m + 1)}{m!}$$

C'est un élément de $\mathbb{Q}[[t , Y]]$: ses coefficients sont des nombres rationnels. Lorsque $t \in \mathbb{Z}_p$, les $\binom{t}{m}$ appartiennent aussi à $\mathbb{Z}_p$, et $(1 + Y)^t$ converge pour $\mathrm{ord}(Y) > 0$, c'est d'ailleurs la puissance "t-ième" de $1 + Y$ en un sens évident.

Formons maintenant le produit infini :

$$F(t , Y) = H(t , Y).H\left(\frac{t^p - t}{p}, Y^p\right).H\left(\frac{t^{p^2} - t^p}{p^2} , Y^{p^2}\right) \ldots \tag{17}$$

c'est-à-dire :

$$F(t , Y) = (1 + Y)^t \, (1 + Y^p)^{\frac{t^p - t}{p}} \, (1 + Y^{p^2})^{\frac{t^{p^2} - t^p}{p^2}} \ldots \tag{18}$$

On voit tout de suite que ce produit infini converge dans $\mathbb{Q}[[t , Y]]$.

LEMME. - Les coefficients de la série formelle F sont dans $\mathbb{Z}_p$.

On calcule $F(t^p , Y^p)/F(t , Y)^p$, et l'on trouve $(1 + Y^p)^t/(1 + Y)^{pt}$. Mais on voit facilement que $(1 + Y^p)/(1 + Y)^p$ est de la forme $1 + pZ$, où Z est une série sans terme constant à coefficients dans $\mathbb{Z}_p$; on en déduit que $(1 + pZ)^t$ est du même type $1 + pZ'$ (utiliser les propriétés de divisibilité des coefficients binômiaux). La relation $F(t^p , Y^p)/F(t , Y)^p = 1 + pZ'$ montre alors que les coefficients de F appartiennent à $\mathbb{Z}_p$ d'après un critère de DWORK ([3], lemme 1).

[On peut aussi démontrer le lemme en exprimant la fonction F au moyen de l'exponentielle de Artin-Hasse.]

Développons F en série par rapport à Y :

$$F(t , Y) = \sum_{m=0}^{\infty} B_m(t).Y^m \quad . \tag{19}$$

On voit tout de suite que B_m est un polynôme de degré $\leq m$ en t . On a donc :

$$F(t , Y) = \sum_{m=0}^{\infty} t^m \alpha_m(Y) \quad , \tag{20}$$

où $\alpha_m(Y)$ est une série formelle commençant par un terme de degré $\geq m$ et à coefficients dans $\mathbb{Z}_p$.

Choisissons maintenant une fois pour toutes une racine primitive p-ième de l'unité $\varepsilon = 1 + \lambda$. On a $\mathrm{ord}(\lambda) = 1/(p - 1)$, on le sait. Posons :

$$\Theta(t) = F(t , \lambda) = \sum_{m=0}^{\infty} \beta_m t^m \ , \quad \text{avec} \quad \beta_m = \alpha_m(\lambda) \quad . \tag{21}$$

On a :

(22) $\quad \mathrm{ord}(\beta_m) \geqslant m/(p-1)$, puisque $\alpha_m(Y)$ commence par Y^m .

La série θ converge donc dans le disque $\mathrm{ord}(t) > -1/(p-1)$.

Soit maintenant $t' \in \underset{\sim}{F}_{p^s} \subset K$, et soit t le représentant multiplicatif de t' dans Ω . On a $t^{p^s} = t$. Si l'on pose $t + t^p + \ldots + t^{p^{s-1}} = \mathrm{Tr}(t)$, l'élément $\mathrm{Tr}(t)$ appartient à $\underset{\sim}{Z}_p$. De plus, on a l'égalité :

(23) $\quad (1+Y)^{\mathrm{Tr}(t)} = F(t, Y).F(t^p, Y) \ldots F(t^{p^{s-1}}, Y)$,

comme on le constate tout de suite. Les deux membres de cette égalité sont des séries entières à coefficients dans Λ ; on peut donc substituer λ à Y , et l'on trouve l'égalité :

(24) $\quad \varepsilon^{\mathrm{Tr}(t)} = \theta(t).\theta(t^p) \ldots \theta(t^{p^{s-1}})$,

où le membre de gauche signifie que l'on élève ε à la puissance $\mathrm{Tr}(t)$-ième, ce qui a un sens puisque $\mathrm{Tr}(t) \in \underset{\sim}{Z}_p$. Comme $\varepsilon^p = 1$, on peut réduire $\mathrm{Tr}(t)$ mod p , et l'on obtient

(25) $\quad \mathrm{Tr}(t') = t' + t'^p + \ldots + t'^{p^{s-1}}$,

la trace étant celle définie par l'extension $\underset{\sim}{F}_{p^s}/\underset{\sim}{F}_p$. L'application $t' \longrightarrow \varepsilon^{\mathrm{Tr}(t')}$ est un caractère additif non trivial du corps $\underset{\sim}{F}_{p^s}$. En résumé :

PROPOSITION 3. - Pour tout entier $s \geqslant 1$, le caractère additif $\varepsilon^{\mathrm{Tr}(t')}$ peut s'écrire sous la forme $\theta(t).\theta(t^p) \ldots \theta(t^{p^{s-1}})$, où t est le représentant multiplicatif de t' , et où θ est une série entière à coefficients dans Ω vérifiant (22).

En fait, les coefficients de θ appartiennent à l'anneau $\underset{\sim}{Z}_p[\varepsilon]$.

4. Traces et déterminants de certaines matrices infinies.

Soit L un corps, et soit n un entier. Si $u = (u_1, \ldots, u_n)$ est un élément de $\underset{\sim}{Z}^n$, on notera X^u le monôme $X_1^{u_1} \ldots X_n^{u_n}$ en les n indéterminées $X = (X_1, \ldots, X_n)$; on dira que u est $\geqslant 0$ si $u_i \geqslant 0$ pour tout i ; on posera $c(u) = \sum u_i$.

Soit $E = L[[X]]$ l'anneau des séries formelles en $X_1, \ldots, X_n$ à coefficients dans L ; à tout $G \in E$, on associe l'endomorphisme $\varphi \longrightarrow G.\varphi$ de E qu'on notera encore G . D'autre part, si q est un entier $\geqslant 2$, on définit un endomorphisme ψ_q de E par la formule :

(26) $$\Psi_q\Big(\sum_{u\geqslant 0} a_u X^u\Big) = \sum_{u\geqslant 0} a_{qu} X^u \quad .$$

Si $G = \sum_{v\geqslant 0} g_v X^v$, l'endomorphisme $\Psi_q \circ G$ de E est représenté par la matrice infinie $\Psi_{q,G}(u , v) = g_{qv-u}$. On notera les formules :

(27) $$\Psi_q \circ \Psi_{q'} = \Psi_{qq'}$$

(28) $$G \circ \Psi_q = \Psi_q \circ G_q , \qquad \text{avec } G_q(X) = G(X^q) \quad .$$

On va appliquer ce qui précède au cas où $L = \Omega$, et où la série $G = \sum_{v\geqslant 0} g_v X^v$ vérifie la condition suivante :

(29). - Il existe une constante $M > 0$ telle que $\mathrm{ord}(g_v) \geqslant M.c(v)$.

Si G_1 et G_2 vérifient (29) il en est de même de leur produit, ainsi que de $G_1(X^h)$ pour tout entier h .

PROPOSITION 4. - Supposons que G vérifie (29). Alors pour tout entier $s \geqslant 1$, la série qui donne la trace de la matrice $(\Psi_{q,G})^s$ est convergente, et si l'on désigne sa somme par $\mathrm{Tr}(\Psi^s)$, on a :

(30) $$(q^s - 1)^n.\mathrm{Tr}(\Psi^s) = \sum_{x^{q^s-1}=1} G(x).G(x^q) \ldots G(x^{q^{s-1}}) \quad .$$

[Ici encore, x désigne un système $(x_1 , \ldots , x_n)$, $x_i \in \Omega$, et la condition $x^{q^s-1} = 1$ signifie que chacun des x_i est une racine $(q^s - 1)$-ième de l'unité.]

Quitte à remplacer q par q^s , et $G(X)$ par $G(X).G(X^q) \ldots G(X^{q^{s-1}})$, on peut supposer que $s = 1$ (utiliser les formules (27) et (28)). On a alors $\mathrm{Tr}(\Psi) = \sum_{u\geqslant 0} g_{(q-1)u}$, série qui est convergente d'après (29). D'autre part, on vérifie aisément que l'on a :

(31) $$\sum_{x^{q-1}=1} x^v = (q - 1)^n \quad \text{si } q - 1 \text{ divise } v$$

$$= 0 \quad \text{sinon} \quad .$$

On a donc bien $\sum_{x^{q-1}=1} G(x) = (q - 1)^n \sum_{u\geqslant 0} g_{(q-1)u}$,

C. Q. F. D.

Considérons maintenant le déterminant de la matrice $1 - t\Psi$, où t est une indéterminée. Il est défini par le développement usuel :

$$\det(1 - t\Psi) = \sum_{m=0}^{\infty} \gamma_m t^m \qquad (32)$$

avec :

$$\gamma_m = (-1)^m \sum \varepsilon(u , v)\ \Psi(u_1 , v_1) \dots \Psi(u_m , v_m) \qquad (33)$$

les $u_1 , \dots , u_m$ étant distincts, les $v_1 , \dots , v_m$ formant une permutation des u, et $\varepsilon(u , v)$ désignant la signature de cette permutation. Si l'on désigne par $\Psi(U)$ un terme typique de la somme (33), on a, en utilisant (29) :

$$\operatorname{ord}(\Psi(U)) \geqslant M(q - 1) \sum_{i=1}^{i=m} c(u_i) \qquad (34)$$

ce qui montre que $\operatorname{ord}(\Psi(U))$ tend vers $+\infty$, et la série (33) est bien convergente.

PROPOSITION 5. - Supposons que G vérifie (29). Alors :

(i). $\det(1 - t\Psi) = \exp\left\{-\sum_{s=1}^{\infty} \operatorname{Tr}(\Psi^s)\ t^s/s\right\}$;

(ii). La série entière $\det(1 - t\Psi)$ a un rayon de convergence infini.

La formule (i) est bien connue pour les matrices finies ; on se ramène à ce cas en "tronquant" Ψ à un ordre r, et en montrant que, si Ψ_r désigne la matrice $r \times r$ ainsi obtenue, le polynôme $\det(1 - t\Psi_r)$ tend vers $\det(1 - t\Psi)$ pour la topologie de la convergence simple des coefficients.

Pour démontrer (ii), il faut prouver que :

$$\operatorname{ord}(\gamma_m)/m \longrightarrow +\infty \qquad \text{lorsque} \quad m \longrightarrow +\infty \qquad . \qquad (35)$$

Or, d'après (34), on a :

$$\operatorname{ord}(\gamma_m) \geqslant M(q - 1).\inf\Big(\sum_{i=1}^{i=m} c(u_i)\Big) \qquad (36)$$

la borne inférieure étant prise sur toutes les suites $u_1 , \dots , u_m$ formés d'éléments positifs et distincts. Si l'on pose :

$$d_m = \inf\Big(\sum_{i=1}^{i=m} c(u_i)\Big) \qquad (37)$$

tout revient donc à montrer que $d_m/m \longrightarrow +\infty$. Mais on peut ranger les $u \geqslant 0$ en une suite $u_1 , \dots , u_n , \dots$ de telle sorte que $c(u_i) \leqslant c(u_{i+1})$, et il est alors clair que $d_m = \sum_{i=1}^{i=m} c(u_i)$. Comme les $c(u_i)$ tendent vers $+\infty$,

il en est de même de leur moyenne arithmétique, ce qui signifie bien que d_m/m tend vers $+\infty$,

C. Q. F. D.

5. Expression analytique des fonctions Z_V .

On a vu au paragraphe 1 qu'il suffit de considérer le cas où V est une hypersurface dans l'espace affine de dimension n , définie par une seule équation $f(x) = 0$, avec $f \in \underset{\sim}{F}_p[X_1 , \ldots , X_n]$. On peut en outre, retrancher de V les points où l'une des coordonnées est nulle. Le nombre N_s est alors simplement le nombre des solutions communes des équations $f(x) = 0$ et $x^{p^s-1} = 1$.

Fixons un entier $s \geq 1$; pour tout $t' \in \underset{\sim}{F}_{p^s}$, soit $\theta_s(t')$ la racine p-ième de l'unité définie par :

$$\theta_s(t') = \varepsilon^{Tr(t')} = \theta(t).\theta(t^p).\ \ldots\ .\theta(t^{p^{s-1}}) \qquad , \tag{38}$$

(cf. proposition 3). Ecrivons k_s au lieu de $\underset{\sim}{F}_{p^s}$ pour simplifier l'écriture. Du fait que θ_s est un caractère non trivial de k_s , on a :

$$\sum_{x_o \in k_s} \theta_s(x_o.u) = p^s \qquad \text{si } u = 0$$
$$= 0 \qquad \text{si } u \neq 0 \quad . \tag{39}$$

En appliquant ceci à $u = f(x)$, et en sommant, il vient :

$$p^s N_s = (p^s - 1)^n + \sum \theta_s(x_o\, f(x)) \qquad , \tag{40}$$

la somme étant étendue aux $x_o \in k_s^*$ et aux $x \in (k_s^*)^n$.

Ecrivons alors $X_o\, f(X_1 , \ldots , X_n)$ comme somme de monômes $\sum_{i=1}^{\rho} a_i X^{w_i}$, où X désigne maintenant $(X_o , \ldots , X_n)$, et où les a_i appartiennent à $\underset{\sim}{F}_p$. On peut donc écrire (40) sous la forme :

$$p^s N_s = (p^s - 1)^n + \sum_{x^{p^s-1}=1} \prod_{i=1}^{\rho} \theta_s(a_i\, x^{w_i}) \quad . \tag{41}$$

Soit $A_i \in \underset{\sim}{Z}_{p^{w_i}}$ le représentant multiplicatif de a_i . Si celui de x est y , celui de $a_i\, x^{w_i}$ est $A_i\, y^{w_i}$. En combinant (38) et (41) on peut donc écrire :

$$p^s N_s = (p^s - 1)^n + \sum_{x^{p^s-1}=1} \prod_{i=1}^{\rho} \prod_{j=0}^{s-1} \theta(A_i\, x^{p^j w_i}) \quad . \tag{42}$$

Posons maintenant :

$$G(X) = \prod_{i=1}^{\rho} \theta(A_i X^{w_i}) \qquad (43)$$

En portant dans (42), on trouve :

$$p^s N_s = (p^s - 1)^n + \sum_{x^{p^s-1}=1} G(x).G(x^p) \dots G(x^{p^{s-1}}) \qquad (44)$$

En utilisant l'inégalité (22) on voit tout de suite que $\theta(A_i X^{w_i})$ vérifie la condition (29) du paragraphe 4, et il en est donc de même de la série G. En lui appliquant la proposition 4, avec $q = p$, et en portant dans (44), on obtient :

$$p^s N_s = (p^s - 1)^n + (p^s - 1)^{n+1}.\mathrm{Tr}(\Psi^s) \qquad (45)$$

ou encore :

$$p^s N_s = \sum_{i=0}^{n} (-1)^i \binom{n}{i} p^{s(n-i)} + \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} p^{s(n+1-i)} \mathrm{Tr}(\Psi^s) \qquad (46)$$

Posons alors :

$$\Delta(t) = \det(1 - t\Psi) = \exp\left\{ - \sum_{s=1}^{\infty} \mathrm{Tr}(\Psi^s)\, t^s/s \right\} \qquad (47)$$

cf. proposition 5.

En multipliant (46) par t^s/s et en ajoutant les équations ainsi obtenues, on obtient finalement :

$$Z_V(pt) = \prod_{i=0}^{i=n} (1 - p^{n-i} t)^{(-1)^{i+1}\binom{n}{i}} \prod_{i=0}^{i=n+1} \Delta(p^{n+1-i} t)^{(-1)^{i+1}\binom{n+1}{i}} \qquad (48)$$

Comme la série entière Δ converge dans tout le plan Ω (proposition 5), la formule (48) montre bien que $Z_V(t)$ est méromorphe dans tout le plan, ce qui achève la démonstration.

BIBLIOGRAPHIE

[1] BOREL (Émile). - Sur une application d'un théorème de M. Hadamard, Bull. Sc. math., 2e série, t. 18, 1894, p. 22-25.

[2] DELSARTE (Jean). - Nombre de solutions des équations polynômiales sur un corps fini, Séminaire Bourbaki, t. 3, 1950/51, n° 39.

[3] DWORK (Bernard). - Norm residue symbol in local number fields, Abh. Math. Sem. Univ. Hamburg, t. 22, 1958, p. 180-190.

[4] DWORK (Bernard). - On the rationality of the zeta function of an algebraic variety, Amer. J. of Math. (à paraître).

[5] WEIL (André). - Number of solutions of equations in finite fields, Bull. Amer. math. Soc., t. 55, 1949, p. 497-508.