

# SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

## Rationalité des fonctions $\zeta$ 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](http://www.numdam.org/item?id=SB_1958-1960__5__415_0)

© Association des collaborateurs de Nicolas Bourbaki, 1960, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

## RATIONALITÉ DES FONCTIONS $\zeta$ DES VARIÉTÉS ALGÈBRIQUES

par Jean-Pierre SERRE

(d'après Bernard DWORK [4])

### 1. Introduction.

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

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

où  $P$  parcourt l'ensemble des points fermés de  $S$ , et où  $N(P)$  est le nombre d'éléments du corps des restes  $\mathbb{F}(P)$  correspondant. Ce produit converge pour  $\Re(s)$  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  $\mathbb{F}_q$ , corps fini à  $q$  éléments (c'est ce que certains appellent une "variété algébrique définie sur  $\mathbb{F}_q$ "). On a alors  $\mathbb{F}_q \subset \mathbb{F}(P)$ , et si  $\deg(P)$  désigne le degré de cette extension, on a :

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

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

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

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

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

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

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 :

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

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

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

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

$$(6) \quad f(X_1, \dots, X_n) = 0, \text{ à coefficients dans } \underline{\mathbb{F}}_p .$$

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

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

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

$$(8) \quad N_{s,m} = \det(A_{s+i+j}), \quad 0 \leq i \leq m, \quad 0 \leq j \leq m .$$

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  $m \geq 0$  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  $\underline{\mathbb{C}}$ ), 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  $\Omega$ , algébriquement clos, contenant  $\underline{\mathbb{Q}}_p$ , et dont la valeur absolue prolonge celle de  $\underline{\mathbb{Q}}_p$ . Une série

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

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  $\Omega$ . 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 :

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

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  $a_0 = 1$ . Quitte à diminuer encore un peu  $r$ , on a des inégalités :

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

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

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 :

$$(12) \quad B_{s+e} = A_{s+e} + a_1 A_{s+e-1} + \dots + a_e A_s \quad .$$

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 :

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

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

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

D'où :

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

Comme  $k > 1$ , ceci entraîne  $|N_{s,m}| \cdot |N_{s,m}|_p < 1$  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  $\Omega$ , autrement dit est quotient de deux séries entières à coefficients dans  $\Omega$ , 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  $\Omega$ ; c'est un corps algébriquement clos de caractéristique  $p$ ; il contient donc tous les  $\mathbb{F}_p$ . Tout élément de  $K$  a un unique "représentant multiplicatif" dans  $\Omega$ . Les  $\mathbb{F}_p$ représentants multiplicatifs des éléments de  $\mathbb{F}_p$  sont les racines  $(p^s - 1)$ -ièmes de l'unité et 0. On note  $\Lambda$  l'anneau des entiers de  $\Omega$ ; on a  $\Lambda \cap \mathbb{Q}_p = \mathbb{Z}_p$ , anneau des entiers  $p$ -adiques. Enfin, on pose

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

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

Soient  $t$  et  $Y$  deux indéterminées. Considérons la série formelle

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

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

Formons maintenant le produit infini :

$$(17) \quad F(t, Y) = H(t, Y) \cdot H\left(\frac{t^p - t}{p}, Y^p\right) \cdot H\left(\frac{t^{p^2} - t^p}{p^2}, Y^{p^2}\right) \dots$$

c'est-à-dire :

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

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  $\mathbb{Z}_{\underline{p}}$ .

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  $\mathbb{Z}_{\underline{p}}$ ; 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  $\mathbb{Z}_{\underline{p}}$  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  $Y$  :

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

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

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

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

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

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

On a :

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

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

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

$$(23) \quad (1+Y)^{\text{Tr}(t)} = F(t, Y) \cdot F(t^p, Y) \dots F(t^{p^{s-1}}, Y),$$

comme on le constate tout de suite. Les deux membres de cette égalité sont des séries entières à coefficients dans  $\mathbb{Z}$ ; on peut donc substituer  $\lambda$  à  $Y$ , et l'on trouve l'égalité :

$$(24) \quad \varepsilon^{\text{Tr}(t)} = \Theta(t) \cdot \Theta(t^p) \dots \Theta(t^{p^{s-1}}),$$

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

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

la trace étant celle définie par l'extension  $\mathbb{F}_s/\mathbb{F}_p$ . L'application

$t' \rightarrow \varepsilon^{\text{Tr}(t')}$  est un caractère additif non trivial du corps  $\mathbb{F}_s$ . En résumé :

PROPOSITION 3. - Pour tout entier  $s \geq 1$ , le caractère additif  $\varepsilon^{\text{Tr}(t')}$  peut s'écrire sous la forme  $\Theta(t) \cdot \Theta(t^p) \dots \Theta(t^{p^{s-1}})$ , où  $t$  est le représentant multiplicatif de  $t'$ , et où  $\Theta$  est une série entière à coefficients dans  $\mathbb{Z}$  vérifiant (22).

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

#### 4. Traces et déterminants de certaines matrices infinies.

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

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

$$(26) \quad \Psi_q \left( \sum_{u \geq 0} a_u X^u \right) = \sum_{u \geq 0} a_{qu} X^u \quad .$$

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

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

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

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

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

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  $s \geq 1$ , la série qui donne la trace de la matrice  $(\Psi_{q,G})^s$  est convergente, et si l'on désigne sa somme par  $\text{Tr}(\Psi^s)$ , on a :

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

[Ici encore,  $x$  désigne un système  $(x_1, \dots, x_n)$ ,  $x_i \in \Omega$ , 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  $G(X) \cdot G(X^q) \dots G(X^{q^{s-1}})$ , on peut supposer que  $s = 1$  (utiliser les formules (27) et (28)). On a alors  $\text{Tr}(\Psi) = \sum_{u \geq 0} g_{(q-1)u}$ , série qui est convergente d'après (29). D'autre part, on vérifie aisément que l'on a :

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

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

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

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 :

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

avec :

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

les  $u_1, \dots, u_m$  étant distincts, les  $v_1, \dots, v_m$  formant une permutation des  $u$ , et  $\xi(u, v)$  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) :

$$(34) \quad \text{ord}(\Psi(U)) \gg M(q-1) \sum_{i=1}^{i=m} c(u_i) \quad ,$$

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

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

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

(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"  $\Psi$  à un ordre  $r$ , et en montrant que, si  $\Psi_r$  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 :

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

Or, d'après (34), on a :

$$(36) \quad \text{ord}(\gamma_m) \gg M(q-1) \cdot \inf\left(\sum_{i=1}^{i=m} c(u_i)\right) \quad ,$$

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

$$(37) \quad d_m = \inf\left(\sum_{i=1}^{i=m} c(u_i)\right) \quad ,$$

tout revient donc à montrer que  $d_m/m \rightarrow +\infty$ . Mais on peut ranger les  $u \geq 0$  en une suite  $u_1, \dots, u_n, \dots$  de telle sorte que  $c(u_i) \leq c(u_{i+1})$ , 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  $f \in \mathbb{F}_p[X_1, \dots, X_n]$ . 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  $t' \in \mathbb{F}_{p^s}$ , soit  $\theta_s(t')$  la racine  $p$ -ième de l'unité définie par :

$$(38) \quad \theta_s(t') = \xi^{\text{Tr}(t')} = \theta(t) \cdot \theta(t^p) \cdot \dots \cdot \theta(t^{p^{s-1}}),$$

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

$$(39) \quad \sum_{x_0 \in k_s} \theta_s(x_0 \cdot u) = p^s \quad \text{si } u = 0 \\ = 0 \quad \text{si } u \neq 0.$$

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

$$(40) \quad p^s N_s = (p^s - 1)^n + \sum \theta_s(x_0 f(x)),$$

la somme étant étendue aux  $x_0 \in k_s^*$  et aux  $x \in (k_s^*)^n$ .

Ecrivons alors  $X_0 f(X_1, \dots, X_n)$  comme somme de monômes  $\sum_{i=1}^p a_i X^{w_i}$ , où  $X$  désigne maintenant  $(X_0, \dots, X_n)$ , et où les  $a_i$  appartiennent à  $\mathbb{F}_p$ . On peut donc écrire (40) sous la forme :

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

Soit  $A_i \in \mathbb{Z}_{p^i}$  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 :

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

Posons maintenant :

$$(43) \quad G(X) = \prod_{i=1}^p \theta(A_i X^{w_i}) \quad .$$

En portant dans (42), on trouve :

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

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.:

$$(45) \quad p^s N_s = (p^s - 1)^n + (p^s - 1)^{n+1} \cdot \text{Tr}(\Psi^s) \quad ,$$

ou encore :

$$(46) \quad p^s N_s = \sum_{i=0}^n (-1)^i \binom{n}{i} \cdot p^{s(n-i)} + \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} p^{s(n+1-i)} \text{Tr}(\Psi^s) \quad .$$

Posons alors :

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

cf. proposition 5.

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

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

Comme la série entière  $\Delta$  converge dans tout le plan  $\Omega$  (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.
-