Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 19 (1973)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI
Autor: Joly, Jean-René
Kapitel: §2. Rationalité des fonctions zêta
DOI: https://doi.org/10.5169/seals-46287

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 17.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

k_2 et conjuguées sur k, a pour fonction zêta $1/(1-t)(1-qt)(1+qt)$, fraction rationnelle qui admet, dans le disque $|t| < q^{-1/2}$, les *deux* pôles $t = q^{-1}$ et $t = -q^{-1}$.

§ **2.** *Rationalité des fonctions zêta.*

2.1. THÉORÈME 2 (théorème de Dwork). — *Quel que soit V, ensemble algébrique défini sur k, $Z(V; t)$ est une fraction rationnelle en t.*

Démonstration. — Soient $\overline{\mathbf{Q}}_p$ la clôture algébrique du corps p-adique $\mathbf{Q}_p$, Ω le complété p-adique de $\overline{\mathbf{Q}}_p$, ord: $\Omega^* \to \mathbf{Q}$, la valuation p-adique de Ω, normalisée par ord $(p) = 1$, et $|\,.\,|_p$: $\Omega \to \mathbf{R}$, la valeur absolue p-adique de Ω, normalisée par $|p|_p = p^{-1}$; Ω est un corps algébriquement clos, complet pour $|\,.\,|_p$: c'est l'analogue p-adique de $\mathbf{C}$. Soit maintenant R un nombre réel positif (ou $+\infty$), et soit D le « disque » de Ω défini par $|t|_p < R$. Une fonction (définie dans une partie de Ω, à valeurs dans $\Omega \cup \{\infty\}$) sera dite *holomorphe dans D* si elle est représentable dans ce disque comme somme d'une série entière convergente; elle sera dite *méromorphe dans D* si elle est égale dans ce disque au quotient de deux fonctions holomorphes. Cela étant, la démonstration du théorème 2 repose essentiellement sur le résultat suivant:

PROPOSITION 1. — *$Z(V; t)$ est méromorphe dans Ω tout entier.*

Indiquons le principe de la démonstration (d'après Dwork (1960), et Serre (1959)). La formule (1.3.4) montre que si V_1 et V_2 sont deux sous-ensembles algébriques d'un même ensemble algébrique, et si on pose $V_3 = V_1 \cup V_2$, $V_4 = V_1 \cap V_2$, les fonctions zêta de ces quatre ensembles algébriques sont liées par $Z(V_1; t)\, Z(V_2; t) = Z(V_3; t)\, Z(V_4; t)$ (remarquer qu'on a, avec des notations évidentes, $N_{1,m} + N_{2,m} = N_{3,m} + N_{4,m}$). Un argument combinatoire simple prouve alors qu'on peut se ramener au cas où V est une hypersurface affine d'équation $F(X_1, \ldots, X_n) = \sum_{\mathbf{u} \in U} a_{\mathbf{u}} X^{\mathbf{u}} = 0$ (notation analogue à celle du chapitre 7, section 2.2), et qu'on ne modifie pas le problème en remplaçant $Z(V; t)$ par $Z^*(V; t) = \exp\left(\sum_{m \geq 1} N_m^* t^m / m\right)$, N_m^* désignant le nombre de points $\mathbf{x} = (x_1, \ldots, x_n) \in V$, rationnels sur k_m et tels que $x_1 x_2 \ldots x_n \neq 0$. Soit β_m un caractère additif non trivial de k_m, *à valeurs dans Ω* (*); un calcul semblable à celui fait au chapitre 5, section 1.3, montre qu'on a

*) C'est-à-dire un homomorphisme non trivial $k_m{}^+ \to \Omega^*$.

$$(2.1.1) \qquad q^m N_m^* = (q^m - 1)^n + \sum_{\mathbf{x}} \beta_m(x_0 F(x_1, \ldots, x_n)),$$

la sommation étant étendue à tous les $\mathbf{x} = (x_0, \ldots, x_n) \in (k_m^*)^{n+1}$.

On va transformer le second membre de (2.1.1). Soit ζ une racine primitive p-ième de l'unité dans Ω, notons Tr_m la trace dans l'extension $k_m/\mathbf{F}_p$, et prenons pour β_m (comme d'habitude) le caractère défini par

$$\beta_m(y) = \zeta^{Tr_m(y)} = \zeta^{y+y^p+\ldots+y^{p^{fm-1}}}$$

($y \in k_m$). Ce caractère peut se « factoriser » grâce au résultat suivant:

LEMME 1. — *Il existe une fonction $B(t)$ holomorphe dans le disque* ord $(t) > -1/(p-1)$ *de Ω, et possédant les deux propriétés ci-dessous:*

(i) *Si $b_0 + b_1 t + \ldots + b_m t^m + \ldots$ est le développement en série entière de $B(t)$ dans ce disque, on a $b_0 = 1$, et* ord $(b_m) \geqslant m/(p-1)$ *pour tout m.*

(ii) *Si on identifie le corps résiduel de Ω à $\bar{k}$, et si, pour tout $y \in k_m^*$, on désigne par $\hat{y}$ l'unique racine (q^m-1)-ième de l'unité contenue dans Ω et ayant y comme image résiduelle dans $k_m \subset \bar{k}$, on a*

$$(2.1.2) \qquad \beta_m(y) = B(\hat{y})\, B(\hat{y}^p) \ldots B(\hat{y}^{p^{fm-1}}).$$

Une telle fonction $B(t)$ peut se construire directement (voir Serre (1959), pp. 4-5, ou Dwork (1960), pp. 634-636); on peut aussi la définir à partir de l'exponentielle d'Artin-Hasse (voir Dwork (1960), p. 636; pour les propriétés de l'exponentielle d'Artin-Hasse, voir par exemple Yamamoto (1959)) ou même à partir de l'exponentielle p-adique ordinaire: en fait, si $\pi \in \Omega$ est tel que $\pi^p = -p$, on peut prendre $B(t) = \exp(\pi t - \pi t^p)$.

Cela étant, (2.1.1) peut s'écrire successivement

$$q^m N_m^* = (q^m - 1)^n + \sum_{\mathbf{x}} \prod_{\mathbf{u} \in U} \beta_m(a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}'})$$

(pour la notation $X^{\mathbf{u}'}$, voir chap. 7, sect. 2.2), puis, compte tenu de (2.1.2),

$$(2.1.3) \qquad q^m N_m^* = (q^m - 1)^n + \sum_{\mathbf{x}} \prod_{\mathbf{u} \in U} \prod_{j=0}^{fm-1} B(\hat{a}_{\mathbf{u}} \hat{\mathbf{x}}^{\mathbf{u}' p^j})$$

($\hat{\mathbf{x}}$ signifie évidemment $(\hat{x}_0, \ldots, \hat{x}_n)$; si $a_{\mathbf{u}} = 0$, $\hat{a}_{\mathbf{u}}$ vaut par définition 0; enfin, la sommation est étendue à tous les $\mathbf{x} \in (k_m^*)^{n+1}$). Ici, faisons un changement de notation: pour tout $y \in k_m^*$, écrivons y au lieu de $\hat{y}$ (ce qui revient à identifier les éléments y de k_m^* avec leurs « représentants multi-

plicatifs » $\hat{y}$ dans Ω); notons par ailleurs T_m le groupe des racines (q^m-1)-ièmes de l'unité dans Ω. La relation (2.1.3) devient

$$(2.1.4) \qquad q^m N_m^* = (q^m-1)^n + \sum_{\mathbf{x}\in T_m^{n+1}} \prod_{\mathbf{u}\in U} \prod_{j=0}^{fm-1} B(a_{\mathbf{u}}\mathbf{x}^{\mathbf{u}'p^j}).$$

Posons alors $C(t) = \prod_{i=0}^{f-1} B(t^{p^i})$ (si on a pris $B(t) = \exp(\pi t - \pi t^p)$, on a tout simplement $C(t) = \exp(\pi t - \pi t^q)$); on vérifie immédiatement (à l'aide de la partie (i) du lemme 1) que $C(t)$ est elle-même holomorphe dans le disque $\operatorname{ord}(t) > -1/(p-1)$ de Ω, et que son développement en série entière $c_0 + c_1 t + \ldots + c_m t^m + \ldots$ dans ce disque satisfait à

$$(2.1.5) \qquad c_0 = 1\ ; \quad \operatorname{ord}(c_m) \geqslant m/(p-1) \quad \text{pour tout } m\ ;$$

comme $a_{\mathbf{u}}^q = a_{\mathbf{u}}$ pour tout $\mathbf{u}\in U$ (le polynôme F est à coefficients dans $k = k_1$), la relation (2.1.4) peut s'écrire

$$(2.1.6) \qquad q^m N_m^* = (q^m-1)^n + \sum_{\mathbf{x}\in T_m^{n+1}} \prod_{\mathbf{u}\in U} \prod_{j=0}^{m-1} C(a_{\mathbf{u}}\mathbf{x}^{\mathbf{u}'q^j}).$$

Introduisons alors la série formelle à $n+1$ variables

$$G(X) = \prod_{\mathbf{u}\in U} C(a_{\mathbf{u}}X^{\mathbf{u}'}) = \sum g_{\mathbf{v}}X^{\mathbf{v}}$$

($\mathbf{v}$ parcourant $\mathbf{N}^{n+1}$). La relation (2.1.6) devient

$$(2.1.7) \qquad q^m N_m^* = (q^m-1)^n + \sum_{\mathbf{x}\in T_m^{n+1}} G(\mathbf{x})\, G(\mathbf{x}^q) \ldots G(\mathbf{x}^{q^{m-1}}),$$

et (2.1.5) permet d'autre part de vérifier que $G(X)$ possède la propriété suivante:

(2.1.8) *Il existe un nombre réel $M > 0$ tel que pour tout $\mathbf{v} = (v_0, \ldots, v_n)$, on ait* $\operatorname{ord}(g_{\mathbf{v}}) \geqslant M(v_0 + \ldots + v_n)$.

Soit alors E l'anneau de séries formelles à $n+1$ variables $\Omega[[X]]$, considéré comme espace vectoriel sur Ω, et définissons de la façon suivante deux endomorphismes Φ et Ψ de E: si $H(X) = \sum h_{\mathbf{v}}X^{\mathbf{v}}$ est un élément quelconque de E, on a $\Phi(H) = \sum h_{q\mathbf{v}}X^{\mathbf{v}}$, et $\Psi(H) = \Phi(GH)$; pour $m \geqslant 1$, soit également Ψ^m le m-ième itéré de Ψ. Alors

LEMME 2. — (i) *La série qui donne la trace $\operatorname{Tr}(\Psi^m)$ de la matrice (infinie) de Ψ^m par rapport aux $X^{\mathbf{v}}$ ($\mathbf{v}\in\mathbf{N}^{n+1}$) est convergente dans Ω et on a*

$$(2.1.9) \qquad (q^m-1)^{n+1}\, Tr(\Psi^m) = \sum_{\mathbf{x}\in T_m^{n+1}} G(\mathbf{x})\, G(\mathbf{x}^q) \ldots G(\mathbf{x}^{q^m-1}).$$

(ii) *Le déterminant caractéristique de Ψ est donné par*

$$(2.1.10) \qquad \text{dét}\,(1-t\Psi) = \exp\Big(-\sum_{m\geq 1} Tr(\Psi^m)\, t^m/m\Big).$$

(iii) *Enfin, $\Delta(t) = \text{dét}\,(1-t\Psi)$ est une fonction holomorphe dans Ω tout entier.*

Pour une démonstration de ce lemme, voir Serre (1959), pp. 7-9 (la démonstration utilise essentiellement la propriété (2.1.8) des coefficients de $G(X)$; la partie (i) du lemme est presque immédiate; la partie (ii) généralise une formule bien connue en dimension finie).

Démontrons alors la proposition 1. Les relations (2.1.7) et (2.1.9) donnent

$$q^m N_m^* = (q^m-1)^n + (q^m-1)^{n+1}\, Tr(\Psi^m);$$

si on développe $(q^m-1)^n$ et $(q^m-1)^{n+1}$ par la formule du binôme et si on utilise la définition de $Z^*(V;t)$ et la formule (2.1.10) (voir le lemme 2, (ii) et (iii)), on trouve

$$(2.1.11) \qquad Z^*(V;t) = K_1(t)\, K_2(t),$$

avec

$$K_1(t) = \prod_{i=0}^{n} (1-p^{n-i-1}t)^{(-1)^{i+1}\binom{n}{i}},$$

$$K_2(t) = \prod_{i=0}^{n+1} \Delta(p^{n-i}t)^{(-1)^{i+1}\binom{n+1}{i}}.$$

$K_1(t)$ est une fraction rationnelle; comme $\Delta(t)$ est holomorphe dans Ω tout entier (lemme 2, (iii)), $K_2(t)$ est évidemment méromorphe dans Ω tout entier; (2.1.11) montre alors que $Z^*(V;t)$ est elle-même méromorphe dans Ω tout entier, et la proposition 1 est établie.

La démonstration du théorème 2 utilise également le résultat suivant:

PROPOSITION 2 (critère de rationalité de Dwork). — *Soit $F(t)$ une série formelle en t à coefficients entiers rationnels, et supposons qu'il existe deux nombres réels positifs R et R_p tels que* (i) *$F(t)$ soit méromorphe dans le disque $|t| < R$ de $\mathbf{C}$;* (ii) *$F(t)$ soit méromorphe dans le disque $|t|_p < R_p$ de Ω;* (iii) *$RR_p > 1$. Alors $F(t)$ est une fraction rationnelle.*

On peut supposer $R_p \geqslant 1$. Si $R_p = 1$ (et par conséquent $R > 1$), on retombe sur le classique *critère de Borel* (voir Borel (1894)). Il suffit donc d'examiner le cas où $R_p > 1$. Si alors $F(t) = a_0 + a_1 t + \ldots + a_m t^m + \ldots$, et si on pose pour tout $h \geqslant 1$

$$D_{m,h} = \text{dét}\,(a_{m+i+j})_{0 \leqq i,j < h},$$

le principe de la démonstration consiste à déduire de (i), (ii) et (iii) l'existence d'un entier h tel que $|D_{m,h}|\,|D_{m,h}|_p < 1$ pour tout m suffisamment grand; comme $D_{m,h}$ est un entier, ceci n'est possible que si $D_{m,h} = 0$ pour m suffisamment grand, donc si, à partir d'un certain rang, les a_m satisfont à une relation de récurrence linéaire de longueur h: mais ceci équivaut à dire que $F(t)$ est une fraction rationnelle. Pour les détails de la démonstration, voir par exemple Serre (1959), pp. 2-4.

Cela étant, le théorème 2 est immédiat: d'après la section 1.4, il existe un entier n tel que $Z(V;t)$ soit holomorphe dans le disque $|t| < q^{-n}$ de $\mathbf{C}$; posons $R = q^{-n}$ et (par exemple) $R_p = q^{n+1}$; on a $RR_p = q > 1$, et $Z(V;t)$ est évidemment méromorphe dans le disque $|t|_p < R_p$ de Ω (prop. 1); la proposition 2 est donc applicable à $Z(V;t)$, qui est effectivement une fraction rationnelle, C.Q.F.D.

2.2. On sait (voir Fatou (1906)) que si $F(t)$ est une fraction rationnelle en t à coefficients dans $\mathbf{Q}$, si $F(0) = 1$, et si le développement en série entière de $F(t)$ a tous ses coefficients *entiers*, alors les zéros et les pôles de $F(t)$ sont des inverses d'entiers algébriques. Ceci s'applique à $Z(V;t)$ et montre qu'on peut écrire

$$Z(V;t) = \prod_{i=1}^{r} (1-\alpha_i t) / \prod_{j=1}^{s} (1-\beta_j t), \tag{2.2.1}$$

les α_i et les β_j étant des entiers algébriques (respectivement les inverses des zéros et des pôles de $Z(V;t)$). Prenant les logarithmes des deux membres et utilisant la formule (1.3.4), on arrive alors au résultat suivant:

COROLLAIRE 1. — *Il existe deux familles* $(\alpha_i)_{1 \leqq i \leqq r}$ *et* $(\beta_j)_{1 \leqq j \leqq s}$ *d'entiers algébriques telles que pour tout* $m \geqslant 1$, *on ait*

$$N_m = \beta_1{}^m + \ldots + \beta_s{}^m - \alpha_1{}^m - \ldots - \alpha_r{}^m. \tag{2.2.2}$$

Remarquons qu'inversement, si V est un ensemble algébrique défini sur k et si $(\alpha_i)_{1 \leqq i \leqq r}$, $(\beta_j)_{1 \leqq j \leqq s}$ sont deux familles d'entiers algébriques telles

qu'on ait (2.2.2) pour tout $m \geqslant 1$, alors la fonction zêta de V est donnée par (2.2.1): on utilisera cette remarque à plusieurs reprises aux paragraphes 3, 4 et 5.

§ 3. *Fonction zêta d'une courbe projective non singulière.*

3.1. Si V est une courbe projective non singulière définie sur k, la fonction $Z(V;t)$ est décrite avec précision par le théorème suivant, dû à Weil (1940, 1948) (voir aussi [**19**], chap. VII, p. 130):

THÉORÈME 3. — *Si V est une courbe projective non singulière de genre g définie sur k, on a*

$$Z(V;t) = P(t)/(1-t)(1-qt), \tag{3.1.1}$$

P étant un polynôme à coefficients entiers rationnels vérifiant les propriétés suivantes :

(i) *Le degré de P est égal à $2g$; son coefficient dominant est égal à q^g et son terme constant à* 1.

(ii) *P satisfait à l'équation fonctionnelle*

$$P(1/qt) = q^{-g}t^{-2g}P(t). \tag{3.1.2}$$

(iii) *Les zéros de P (qui sont des inverses d'entiers algébriques, d'après* (i)*), ont tous pour module $q^{-1/2}$.*

Démonstration. — On utilise essentiellement le théorème 3 du chapitre 8 et le résultat suivant:

PROPOSITION 3. — *Mêmes hypothèses que dans le théorème* 3 *; la fonction zêta de V satisfait à l'équation fonctionnelle*

$$Z(V;1/qt) = q^{1-g}t^{2-2g}Z(V;t). \tag{3.1.3}$$

Prouvons cette proposition (et convenons, pour simplifier, d'écrire $Z(t)$ au lieu de $Z(V;t)$, et de dire systématiquement *diviseur* au lieu de *diviseur rationnel sur k*). La formule (1.3.1) montre que $Z(t) = \sum_{m \geqslant 0} D_m t^m$, D_m désignant ici (puisque V est une courbe) le nombre de diviseurs positifs de degré m sur V. Mais V possède un diviseur $\mathfrak{m}_0$ (non nécessairement positif) de degré 1 (chap. 8, th. 3, cor. 2); d'autre part, les diviseurs *positifs* de degré g sur V forment un ensemble fini, et l'équivalence linéaire entre divi-