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: §1. Définitions, propriétés élémentaires.
DOI: https://doi.org/10.5169/seals-46287

nitions de $Z(V; t)$, l'énoncé (mais non la démonstration) du théorème 2, et le corollaire 1 de ce théorème 2 (on y utilise également les résultats des chapitres 5 et 6).

§ 1. *Definitions, propriétés élémentaires.*

1.1. Soit V un ensemble algébrique (affine ou projectif) défini sur k, et soit $\mathbf{M}$ l'ensemble des cycles de dimension 0, premiers rationnels sur k, et portés par V (voir [**15**], chap. I, §§ 9.2 et 9.3); rappelons qu'un tel cycle $\mathfrak{m}$ est une combinaison linéaire formelle $\mathbf{x}_1 + \ldots + \mathbf{x}_m$ de points de V (algébriques sur k) satisfaisant aux deux conditions suivantes:

(i) $k(\mathbf{x}_1) = \ldots = k(\mathbf{x}_m) = k_m$;

(ii) les $\mathbf{x}_j$ $(1 \leqslant j \leqslant m)$ sont permutés transitivement par le groupe de Galois de k_m/k;

l'entier m s'appelle *degré de* $\mathfrak{m}$, on le note $\deg(\mathfrak{m})$; l'entier $q^{\deg(\mathfrak{m})} = \mathrm{card}(k_m)$ est noté $N\mathfrak{m}$; cela étant:

DÉFINITION 1. — *On appelle fonction zêta (« minuscule ») de V la fonction d'une variable complexe s définie par*

$$\zeta(V; s) = \prod_{\mathfrak{m} \in \mathbf{M}} 1/(1 - N\mathfrak{m}^{-s}). \tag{1.1.1}$$

(On verra plus loin que ce produit infini converge quand la partie réelle de s est suffisamment grande.)

Si V est une k-variété affine, il existe une bijection canonique de $\mathbf{M}$ sur l'ensemble des idéaux maximaux de l'anneau de coordonnées $A = k[V]$ (conséquence facile du théorème des zéros de Hilbert); faisons l'identification correspondante; si alors $\mathfrak{m} \in \mathbf{M}$, $A/\mathfrak{m}$ est isomorphe à k_m, avec $m = \deg(\mathfrak{m})$, et on a $N\mathfrak{m} = \mathrm{card}(A/\mathfrak{m})$; la définition (1.1.1) de $\zeta(V; s)$ à partir de $A = k[V]$ et de l'ensemble $\mathbf{M}$ des idéaux maximaux de A est dans ce cas entièrement analogue à celle de la fonction $\zeta(K; s)$ d'un corps de nombres K à partir de l'anneau $A = O_K$ des entiers de K et de l'ensemble des idéaux maximaux de A. (Ces deux définitions sont en fait des cas particuliers de la notion générale de fonction zêta d'un schéma de type fini sur $\mathbf{Z}$: voir [**16**], pp. 82-86).

1.2. La relation $N\mathfrak{m} = q^{\deg(\mathfrak{m})}$ incite à faire le changement de variable $t = q^{-s}$ et à poser une seconde définition:

DÉFINITION 2. — *On appelle fonction zêta (« majuscule ») de V la fonction d'une variable complexe t définie par*

$$Z(V;t) = \prod_{\mathfrak{m}\in\mathbf{M}} 1/(1-t^{\deg(\mathfrak{m})}). \tag{1.2.1}$$

(On verra que ce produit infini converge quand $|t|$ est suffisamment petit.)

On a alors évidemment

$$\zeta(V;s) = Z(V;q^{-s}). \tag{1.2.2}$$

1.3. On va transformer la définition (1.2.1) de $Z(V;t)$. Pour tout $j \geqslant 1$, soit d_j le nombre de cycles $\mathfrak{m} \in \mathbf{M}$ tels que $\deg(\mathfrak{m}) = j$: le nombre de points $x \in V$ tels que $[k(\mathbf{x}):k] = j$ est évidemment égal à jd_j. Soit maintenant m un entier $\geqslant 1$; le nombre de points $\mathbf{x} \in V$ rationnels sur k_m (c'est-à-dire tels que $k(\mathbf{x}) \subset k_m$, donc que $[k(\mathbf{x}):k]$ divise m: chap. 1, prop. 4) est alors donné par

$$N_m = \sum_{j|m} jd_j. \tag{1.3.1}$$

D'autre part, l'égalité (1.2.1) peut s'écrire

$$Z(V;t) = \prod_{j\geqq 1} 1/(1-t^j)^{d_j}. \tag{1.3.2}$$

Considérons provisoirement t comme une indéterminée; dans l'anneau de séries formelles $\mathbf{Q}[[t]]$, le produit infini figurant au second membre de (1.3.2) est évidemment convergent, et il est de la forme $1 + tG(t)$, avec $G(t) \in \mathbf{Z}[[t]]$. Si D_j désigne le nombre de cycles positifs de dimension 0 et de degré d rationnels sur k (mais non nécessairement premiers) et portés par V, un calcul facile (analogue à celui qui permet de transformer en série de Dirichlet la fonction zêta de Riemann, supposée définie comme produit « eulérien » infini) montre d'ailleurs qu'on a de façon précise

$$Z(V;t) = 1 + \sum_{m\geqq 1} D_m t^m. \tag{1.3.3}$$

Prenons alors, dans $\mathbf{Q}[[t]]$, les logarithmes des deux membres de (1.3.2); il vient

$$\log Z(V;t) = \sum_{j\geqq 1} \sum_{n\geqq 1} d_j t^{nj}/n,$$

soit, en multipliant par j le numérateur et le dénominateur du terme général, en posant $m = nj$, et en tenant compte de (1.3.1),

$$\log Z(V;t) = \sum_{m \geqq 1} N_m t^m/m .$$

Ainsi:

PROPOSITION 1. — *Considérons $Z(V;t)$ comme élément de $\mathbf{Q}[[t]]$. Alors*

(i) *$Z(V;t)$ appartient à $1 + t\mathbf{Z}[[t]]$, et elle est donnée explicitement par la formule (1.3.3).*

(ii) *Si N_m désigne le nombre de points de V rationnels sur k_m, on a*

$$Z(V;t) = \exp\Big(\sum_{m \geqq 1} N_m t^m/m\Big). \tag{1.3.4}$$

La formule (1.3.4) est plus maniable que la formule (1.2.1), et c'est elle qu'on prend généralement comme *définition* de $Z(V;t)$; $\zeta(V;s)$ est alors *définie* par la formule (1.2.2).

1.4. Considérons à nouveau t comme une variable complexe, et $Z(V;t)$ comme une fonction de variable complexe. Si on suppose V affine, plongé dans $\mathbf{A}_n$, l'entier N_m est majoré par le nombre de points de $\mathbf{A}_n$ rationnels sur k_m; on a donc $N_m \leqslant (q^n)^m = (q^n)^m$, et la série entière $\sum_{m \geqq 1} N_m t^m/m$ admet pour majorante la série entière $\sum_{m \geqq 1} (q^n t)^m/m = \log 1/(1-q^n t)$, qui est holomorphe dans le disque $|t| < q^{-n}$; ainsi, $Z(V;t)$ est holomorphe (au moins) dans le disque $|t| < q^{-n}$. Même raisonnement et même conclusion si V est projectif, plongé dans $\mathbf{P}_n$; on a alors $N_m \leqslant (q^n)^m + (q^{n-1})^m + \ldots + q^m + 1$, et la série $\sum_{m \geqq 1} N_m t^m/m$ admet pour majorante la fonction $\log 1/(1-t)(1-qt)\ldots(1-q^n t)$, qui est holomorphe dans $|t| < q^{-n}$. Compte tenu de (1.2.2), on peut donc énoncer:

PROPOSITION 2. — *Si V désigne un ensemble algébrique défini sur k et plongé dans l'espace affine ou projectif de dimension n sur k, la fonction $Z(V;t)$ (supposée définie par (1.3.4)) est holomorphe (au moins) dans le disque $|t| < q^{-n}$; la fonction $\zeta(V;s)$ est holomorphe (au moins) dans le demi-plan $Re(s) > n$.*

On laisse au lecteur le soin de vérifier, en passant par l'intermédiaire de la formule (1.3.3), que le produit infini (1.2.1) converge pour $|t| < q^{-n}$ (au moins) et que le produit infini (1.1.1) converge alors pour $Re(s) > n$ (au moins). Notons d'autre part que les majorantes introduites ci-dessus ne sont autres que les logarithmes des fonctions zêta de $\mathbf{A}_n$ et $\mathbf{P}_n$; ainsi

PROPOSITION 3. — *Considérons* $\mathbf{A}_n$ *et* $\mathbf{P}_n$ *comme variétés définies sur* k *; alors*

$$Z(\mathbf{A}_n; t) = 1/(1-q^n t) ; \tag{1.4.1}$$

$$Z(\mathbf{P}_n; t) = 1/(1-t)(1-qt)\dots(1-q^n t) . \tag{1.4.2}$$

Si V est une *variété,* le théorème 4 du chapitre 8 permet d'en dire plus:

THÉORÈME 1. — *Soit* V *une variété (affine ou projective) de dimension* r*, définie sur* k*. Alors*

(i) $Z(V; t)$ *est holomorphe dans le disque* $|t| < q^{-r}$.

(ii) *Elle se prolonge analytiquement en une fonction méromorphe dans le disque* $|t| < q^{-r+(1/2)}$.

(iii) *Ainsi prolongée, elle n'admet aucun zéro, et elle a pour seule singularité un pôle simple en* $t = q^{-r}$.

Démonstration. — D'après le chapitre 8 (sect. 4.1, th. 1, pour le cas projectif; sect. 4.3, pour le cas affine), on peut, pour tout $m \geqslant 1$, écrire

$$N_m = (q^m)^r + B_m (q^m)^{r-(1/2)} , \tag{1.4.3}$$

et la suite B_m $(m = 1, 2, \dots)$ est alors *bornée*; posons

$$H(u) = \sum_{m \geqslant 1} B_m u^m / m ;$$

$H(u)$ est holomorphe dans le disque $|u| < 1$, et (1.4.3), joint à (1.3.4), permet d'écrire

$$Z(V; t) = \exp\left(H(q^{r-(1/2)}t)\right)/(1-q^r t) ; \tag{1.4.4}$$

le numérateur et le dénominateur du membre de droite sont holomorphes dans le disque $|t| < q^{-r+(1/2)}$, et le numérateur ne s'y annule évidemment pas; comme par ailleurs le dénominateur ne s'annule dans ce disque qu'en $t = q^{-r}$, qui est un zéro simple, le théorème 1 se trouve établi.

Les assertions (i) et (ii) du théorème 1 restent vraies pour un ensemble algébrique V quelconque (en ce qui concerne (ii), on a déjà annoncé, et on démontrera au paragraphe 2, que $Z(V; t)$ est une fraction rationnelle: elle se prolonge donc analytiquement à $\mathbf{C}$ tout entier !); tel n'est plus le cas pour l'assertion (iii): par exemple, si $q \equiv 3 \pmod 4$, la k-variété projective définie dans $\mathbf{P}_2$ (rapporté à un système de *trois* coordonnées homogènes x, y, z) par l'équation $X^2 + Y^2 = 0$, et qui est formée de deux droites définies sur

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 ${k_m}^+ \to \Omega^*$.