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

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **19 (1973)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **11.07.2024**

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*

(3.1.1) $$Z(V;t) = P(t)/(1-t)(1-qt),$$

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*

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

(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*

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

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 $Z(t) = \sum_{m \geq 0} D_m t^m$, 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 diviseurs partage cet ensemble en classes d'équivalence: on peut donc trouver une famille $\mathfrak{m}_1, \ldots, \mathfrak{m}_h$ de diviseurs positifs de degré g sur V telle que tout diviseur positif $\mathfrak{m}$ de degré g sur V soit linéairement équivalent à un $\mathfrak{m}_j$ $(1 \leqslant j \leqslant h)$ et un seul; et ceci reste d'ailleurs vrai *même si on ne suppose pas* $\mathfrak{m}$ *positif* (en effet, si $\deg(\mathfrak{m}) = g$, le théorème de Riemann-Roch donne $l(\mathfrak{m}) \geqslant 1$, de sorte que tout diviseur $\mathfrak{m}$ de degré g sur V est linéairement équivalent à un diviseur *positif* de degré g sur V).

Pour tout $m \geqslant 0$ et tout j $(1 \leqslant j \leqslant h)$, posons alors

$$\mathfrak{m}_{j,m} = \mathfrak{m}_j + (m-g)\,\mathfrak{m}_0\,. \tag{3.1.4}$$

Il est clair que, quel que soit le diviseur positif $\mathfrak{m}$ sur V, il existe un couple (j, m) et un seul tel que $\mathfrak{m} \sim \mathfrak{m}_{j,m}$ (m étant d'ailleurs égal à $\deg(\mathfrak{m})$). Calculons maintenant D_m; si $D_{j,m}$ est le nombre de diviseurs positifs sur V linéairement équivalents à $\mathfrak{m}_{j,m}$, il résulte de ce qui précède que

$$D_m = \sum_{j=1}^{h} D_{j,m}\,; \tag{3.1.5}$$

par ailleurs, on sait que les diviseurs positifs sur V qui sont linéairement équivalents à un diviseur donné $\mathfrak{n}$ forment un espace projectif de dimension $l(\mathfrak{n}) - 1$ sur k (c'est la série linéaire complète $|\,\mathfrak{n}\,|$ associée à $\mathfrak{n}$); on a donc

$$D_{j,m} = \operatorname{card}(|\mathfrak{m}_{j,m}|) = (q^{l(\mathfrak{m}_{j,m})} - 1)/(q-1)\,. \tag{3.1.6}$$

(1.3.1), (3.1.5) et (3.1.6) donnent ainsi, après multiplication par $q - 1$:

$$(q-1)\,Z(t) = \sum_{m \geqq 0} \sum_{j=1} (q^{l(\mathfrak{m}_{j,m})} - 1)\,t^m\,. \tag{3.1.7}$$

Posons alors

$$F(t) = \sum_{m=0}^{2g-2} \sum_{j=1}^{h} q^{l(\mathfrak{m}_{j,m})} t^m\,, \tag{3.1.8}$$

$$R(t) = -\sum_{m=0}^{2g-2} t^m + h^{-1} \sum_{m \geqq 2g-1} \sum_{j=1}^{h} (q^{l(\mathfrak{m}_{j,m})} - 1)\,t^m\,; \tag{3.1.9}$$

on a évidemment

$$(q-1)\,Z(t) = F(t) + hR(t)\,; \tag{3.1.10}$$

mais le théorème de Riemann-Roch montre que pour $\deg(\mathfrak{m}) = m \geqslant 2g - 1$, on a $l(\mathfrak{m}) = m - g + 1$; ceci permet, dans $R(t)$, de remplacer chaque somme $\sum_{j=1}^{h} (q^{l(\mathfrak{m}_{j,m})} - 1)\, t^m$ par $h\,(q^{m-g+1} - 1)\, t^m$, et donne après sommation de deux séries géométriques

$$(3.1.11) \qquad R(t) = -1/(1-t) + q^g t^{2g-1}/(1-qt)\,.$$

Un calcul direct prouve alors que

$$(3.1.12) \qquad R(1/qt) = q^{1-g} t^{2-2g} R(t)\,.$$

D'autre part, si $\mathfrak{w}$ est un diviseur canonique sur V, le théorème de Riemann-Roch donne

$$l(\mathfrak{m}_{j,m}) = m - g + 1 + l(\mathfrak{w} - \mathfrak{m}_{j,m})\,;$$

en outre, pour toute valeur de m telle que $0 \leqslant m \leqslant 2g - 2$, il est clair que les h nombres $l\,(\mathfrak{w} - \mathfrak{m}_{j,m})\,(1 \leqslant j \leqslant h)$ sont les mêmes, à l'ordre près, que les h nombres $l\,(\mathfrak{m}_{j,2g-2-m})\,(1 \leqslant j \leqslant h)$; il résulte de ces deux remarques (et de la définition (3.1.8) de $F(t)$) que

$$(3.1.13) \qquad F(1/qt) = q^{1-g} t^{2-2g} F(t)\,.$$

Le rapprochement de (3.1.10), (3.1.12) et (3.1.13) donne immédiatement l'équation fonctionnelle (3.1.3), et la proposition 3 se trouve établie.

Démontrons alors le théorème 3. Posons par définition

$$P(t) = (1-t)\,(1-qt)\,Z(t)\,;$$

l'équation fonctionnelle (3.1.3) pour $Z(t)$ (prop. 3) implique l'équation fonctionnelle (3.1.2) pour $P(t)$, ce qui prouve (ii). Les formules (3.1.10), (3.1.8) et (3.1.11) (voir la démonstration de la prop. 3) montrent que $P(t)$ est un polynôme à coefficients entiers: (i) résulte alors de (ii), en ce qui concerne le degré de P et la valeur de son coefficient dominant; et du fait que $P(0) = Z(0) = 1$, en ce qui concerne son terme constant.

Reste à démontrer (iii). On a

$$\log P(t) = \log Z(t) - \log(1-t)\,(1-qt) = \sum_{m \geqq 0} (N_m - 1 - q^m)\, t^m/m\,;$$

le théorème 3 du chapitre 8 montre que la série entière de droite admet pour majorante la série $\sum_{m \geqq 0} 2q^{m/2} t^m$, qui est holomorphe dans le disque $|\,t\,| < q^{-1/2}$ de C; $\log P(t)$ est donc holomorphe dans ce disque, de sorte que $P(t)$ n'admet aucun zéro dans le disque $|\,t\,| < q^{-1/2}$; comme la transformation $t \mapsto 1/qt$ échange l'intérieur et l'extérieur de ce disque, (ii) montre que $P(t)$ n'admet également aucun zéro dans le domaine $|t| > q^{-1/2}$: tous les zéros de $P(t)$ sont donc sur le cercle $|t| = q^{-1/2}$, ce qui prouve (iii) et achève la démonstration du théorème 3.

COROLLAIRE 1. — *Tous les zéros de la fonction $\zeta(V; s)$ sont sur la droite $Re(s) = 1/2$.*

Démonstration. — On a en effet $\zeta(V; s) = Z(V; q^{-s})$, et le changement de variable $t = q^{-s}$ transforme les t de module $q^{-1/2}$ en les s de partie réelle $1/2$.

3.2. Ce corollaire 1 constitue l'analogue géométrique de l'hypothèse de Riemann, et résulte directement du théorème 3 du chapitre 8. Inversement, ce corollaire 1 (ou, ce qui revient au même, la partie (iii) du théorème 3 ci-dessus) implique le théorème 3 du chapitre 8: écrivons en effet $Z(V; t) = P(t)/(1-t)(1-qt)$, et soient α_i $(1 \leqslant i \leqslant 2g)$ les *inverses* des $2g$ zéros de $P(t)$; on a alors $Z(V; t) = (1-\alpha_1 t)\ldots(1-\alpha_{2g}t)/(1-t)(1-qt)$, donc (voir sect. 2.2), $N_m = q^m + 1 - \alpha_1{}^m - \ldots - \alpha_{2g}^m$; pour $m = 1$, ceci permet d'écrire $|q + 1 - N_1| \leqslant |\alpha_1| + \ldots + |\alpha_{2g}|$; si maintenant on suppose que les $2g$ zéros de P ont pour module $q^{-1/2}$, on a $|\alpha_i| = q^{1/2}$ pour $i = 1, \ldots, 2g$, et la dernière inégalité se réduit (puisque $N = N_1$) à

$$|q + 1 - N| \leqslant 2gq^{1/2}:$$

on retrouve bien l'inégalité (3.1.1) du chapitre 8.

3.3. Remarquons pour terminer que dans la démonstration du théorème 3 ci-dessus, la rationalité de $Z(V; t)$ a été établie directement (à l'aide du théorème de Riemann-Roch), indépendamment du théorème 2. Signalons d'autre part que l'entier h qui s'est introduit au cours de la démonstration de la proposition 3 est égal au nombre de classes de diviseurs de degré 0 du corps de fonctions algébriques $k(V)/k$, et qu'on a $P(1) = h$; ainsi, dans le cas géométrique comme dans le cas arithmétique, il y a un rapport étroit entre nombre de classes et comportement de la fonction ζ au point $s = 1$ (à ce sujet, voir par exemple [**19**], chap. VII).

§ **4.** *Conjectures de Weil.*

4.1. Soit maintenant V une variété projective non singulière de type (n, d, r) (voir chap. 8, § 4) définie sur k. Une description de $Z(V; t)$, généralisant le théorème 3 (qui correspond à $r = 1$), est donnée par les énoncés suivants, dits « conjectures de Weil » (voir Weil (1949), p. 507):