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: Chapitre 9 FONCTIONS ZÊTA
DOI: https://doi.org/10.5169/seals-46287

voir Igusa (1949) et Roquette (1953) (voir aussi [**5**], chap. V, §§ 1-5); dans tous les cas, le point essentiel est l'inégalité $\sigma(\xi\xi') > 0$ (inégalité (23), p. 292, dans [**5**], par exemple); pour un commentaire sur cette inégalité (dite « de Castelnuovo »), voir Weil (1954), p. 553. Pour une application aux « sommes exponentielles », voir Weil (1948, b).

§ **4**: la constante $A_1(n, d, r)$ (lemme 1) peut être prise égale à $(2d)^r$ (en fait, elle ne dépend donc pas de n); en revanche, la constante $A_2(n, d, r)$ (lemme 2) et par conséquent la constante $A(n, d, r)$ (th. 4) dépendent de n; on ne sait d'ailleurs pas en général les majorer explicitement, faute de renseignements précis sur le degré $e(n, d, r)$ de l'ensemble algébrique E.

Pour d'autres remarques sur les résultats ci-dessus, voir également le chapitre 9.

CHAPITRE 9

FONCTIONS ZÊTA

Dans ce dernier chapitre, on se donne comme toujours un corps fini k à $q = p^f$ éléments, de clôture algébrique $\bar{k}$; pour tout entier $m \geqslant 1$, k_m désigne l'unique extension de degré m de k contenue dans $\bar{k}$ (chap. 1, § 1). A tout ensemble algébrique V défini sur k, on peut alors associer la série formelle $Z(V; t) = \exp\left(\sum_{m \geqq 1} N_m t^m/m\right)$, où N_m désigne le nombre de points de V rationnels sur k_m, et où t est une indéterminée. Il se trouve que cette série formelle est en fait une fraction rationnelle en t, et que, moyennant des hypothèses convenables sur V, cette fraction rationnelle peut être décrite avec précision. Le paragraphe 1 de ce chapitre énonce diverses définitions équivalentes de $Z(V; t)$, et justifie le nom de « fonction zêta de V » qui lui est attribué. Le paragraphe 2 donne une esquisse de la démonstration de la rationalité de $Z(V; t)$. Le paragraphe 3 montre comment le théorème de Riemann-Roch et le théorème 3 du chapitre 8 permettent d'obtenir une description très complète de $Z(V; t)$ quand V est une courbe projective non singulière. Le paragraphe 4 indique sans démonstration diverses généralisations des résultats du paragraphe 3. Enfin, le paragraphe 5 donne des exemples de calcul explicite de fonctions zêta; ce paragraphe peut d'ailleurs être lu directement après le paragraphe 2: on y utilise uniquement les défi-

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

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

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

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

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 $\mathrm{ord}(t) > -1/(p-1)$ 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

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

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

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

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

$$G(X) = \prod_{u \in U} C(a_u X^{u'}) = \sum g_v X^v$$

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

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

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 $v = (v_0, \ldots, v_n)$, on ait* $\mathrm{ord}(g_v) \geqslant M(v_0 + \ldots + v_n)$.

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 $H(X) = \sum h_v X^v$ est un élément quelconque de E, on a $\Phi(H) = \sum h_{qv} X^v$, 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 $Tr(\Psi^m)$ de la matrice (infinie) de Ψ^m par rapport aux X^v ($v \in \mathbf{N}^{n+1}$) est convergente dans Ω et on a*

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

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

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

(iii) *Enfin, $\Delta(t) = \det(1-t\Psi)$ 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 $h \geqslant 1$

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

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 $(\alpha_i)_{1 \leqslant i \leqslant r}$ et $(\beta_j)_{1 \leqslant j \leqslant s}$ 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 $(\alpha_i)_{1 \leqslant i \leqslant r}$, $(\beta_j)_{1 \leqslant j \leqslant s}$ 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 $Z(t) = \sum_{m \geqq 0} D_m t^m$, 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-

seurs 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 $q - 1$:

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

Posons alors

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

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

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

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

Un calcul direct prouve alors que

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

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

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

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):

(CW1) (Théorème de Lefschetz). — *Il existe* $2r+1$ *familles d'entiers algébriques* $(\alpha_{ji})_{1\leq j\leq B_i}$, $0\leqslant i\leqslant 2r$, *telles qu'en posant, pour chaque* i, $P_i(t)=\prod_{j=1}^{B_i}(1-\alpha_{ji}t)$, *on ait*

$$Z(V;t)=\frac{P_1(t)\,P_3(t)\ldots P_{2r-1}(t)}{P_0(t)\,P_2(t)\ldots P_{2r}(t)}; \tag{4.1.1}$$

de plus, $P_0(t)=1-t$ et $P_{2r}(t)=1-q^rt$.

(CW2) (Equation fonctionnelle). — *Si on pose* $\chi=\sum_{i=0}^{2r}(-1)^i B_i$, *on a*

$$Z(V;1/q^rt)=\pm q^{r\chi/2}t^{\chi}Z(V;t)\,. \tag{4.1.2}$$

(CW3) (« Hypothèse de Riemann »). — *Pour tout couple d'indices* j, i, *on a*

$$|\alpha_{ji}|=q^{i/2}\,. \tag{4.1.3}$$

(CW4) (Rationalité des « polynômes de Weil » P_i). — *Chacun des polynômes* P_i *est à coefficients entiers rationnels, de terme constant égal à* 1.

(CW5) (Interprétation des entiers B_i comme nombres de Betti). — *Si* V *se relève en caractéristique* 0 *(autrement dit, s'il existe un anneau de valuation discrète* $\mathfrak{O}$, *contenu dans* $\mathbf{C}$, *et dont le corps résiduel s'identifie à* k, *et une variété projective non singulière* V_0, *définie sur* $\mathfrak{O}$, *et dont la variété réduite modulo l'idéal maximal de* $\mathfrak{O}$ *s'identifie à* V*), alors les* B_i *sont égaux aux nombres de Betti de* V_0, *considérée comme variété topologique complexe compacte de dimension complexe* r, *donc de dimension réelle* $2r$. *(L'exposant* χ, *dans l'équation fonctionnelle* (4.1.2), *est alors la caractéristique d'Euler-Poincaré de* V_0*).*

On remarquera que, compte tenu de la définition des P_i, (4.1.1) équivaut (voir th. 2, cor. 1 et remarque) à la collection d'égalités

$$N_m=\sum_{i,\,j}(-1)^i\alpha_{ji}^m\quad(m=1,2,\ldots);$$

de même, (4.1.2) équivaut à l'assertion suivante: quel que soit i $(0\leqslant i\leqslant 2r)$, les deux familles $(\alpha_{ji})_{1\leq j\leq B_{2r-i}}$ et $(q^r\alpha_{ji}^{-1})_{1\leq j\leq B}$ sont identiques (à une permutation près).

4.2. L'ensemble de ces conjectures a été démontré par Weil lui-même lorsque V est une *courbe* (th. 3), et lorsque V est une *variété abélienne* (voir

par exemple [9], notamment p. 140). Le cas où V est une *hypersurface* (c'est-à-dire où $r = n - 1$) a été traité par Dwork (1962, 1964; 1966, a) qui a montré, en perfectionnant les méthodes p-adiques de son article de 1960, qu'on a alors

$$(4.2.1) \qquad Z(V;t) = P(t)^{(-1)^n}/(1-t)(1-qt)\dots(1-q^{n-1}t),$$

$P(t)$ étant un polynôme de degré $d^{-1}((d-1)^{n+1} + (-1)^{n+1}(d-1))$: ceci prouve (CW1), (CW2) et (CW5) pour les hypersurfaces.

4.3. Les conjectures (CW1), (CW2) et (CW5) ont été démontrées en toute généralité par Artin et Grothendieck (voir Grothendieck (1964, a; b)) et, de deux manières différentes, par Lubkin (1967, 1968). Le principe de ces démonstrations est la construction, pour les variétés algébriques (ou plus précisément les schémas), d'une cohomologie à coefficients dans un corps K de caractéristique 0 (« cohomologie de Weil »), consistant en la donnée, pour tout $i \geqslant 0$, d'un foncteur H^i de la catégorie des schémas projectifs non singuliers dans la catégorie des espaces vectoriels de dimension finie sur K, cette famille de foncteurs possédant (entre autres) les propriétés suivantes:

(4.3.1) *Si* $\dim(V) = r$, *alors* $H^i(V) = 0$ *pour* $i > 2r$.

(4.3.2) (Formule « des traces », ou « des points fixes », de Lefschetz). — *Si f est un morphisme $V \to V$, et si $f_i = H^i(f)$ est l'endomorphisme correspondant dans $H^i(V)$, alors le nombre d'intersection $i(\Gamma \cdot \Delta)$ du graphe Γ de f avec la diagonale Δ de $V \times V$ est donné par*

$$i(\Gamma \cdot \Delta) = \sum_{i=0}^{2r} (-1)^i \, Tr(f_i).$$

(4.3.3) (Formule de dualité). — *L'espace vectoriel $H^{2r}(V)$ est isomorphe à K (r désignant toujours la dimension de V), et il existe pour tout i tel que $0 \leqslant i \leqslant 2r$ une application bilinéaire $H^i(V) \times H^{2r-i}(V) \to H^{2r}(V) \simeq K$ mettant $H^i(V)$ et $H^{2r-i}(V)$ en dualité.*

(4.3.4) *Si V se relève en caractéristique 0 selon une variété complexe V_0, la « cohomologie de Weil » de V s'identifie à la cohomologie ordinaire de V_0 (à coefficients dans K).*

La « cohomologie de Weil » d'Artin-Grothendieck est la cohomologie l-adique étale, pour laquelle $K = \mathbf{Q}_l$, l désignant n'importe quel nombre premier différent de la caractéristique p du corps de base k; les « cohomologies de Weil » de Lubkin utilisent respectivement comme corps de

coefficients $K = \mathbf{Q}_l$, $l \neq p$ (Lubkin (1967)) et $K = \mathbf{Q}_p$ (Lubkin (1968)). A titre d'exemple, montrons comment la formule (4.1.1) peut se déduire de la formule des traces de Lefschetz: k et V étant fixés, soit f l'endomorphisme de V défini par $f(\mathbf{x}) = \mathbf{x}^{(q)}$ ($\mathbf{x} \in V$; voir chap. 8, § 2) et soit Γ le graphe de f dans $V \times V$; on peut montrer que tous les points du cycle intersection $\Gamma \cdot \Delta$ ont pour multiplicité 1; comme ces points correspondent bijectivement aux points de V invariants par f, donc rationnels sur k, la formule de Lefschetz donne

$$N_1 = \sum_{i=0}^{2r} (-1)^i \, Tr(f_i);$$

appliquant le même raisonnement au corps de base k_m et à l'endomorphisme f^m, on trouve plus généralement, pour tout $m \geqslant 1$,

$$N_m = \sum_{i=0}^{2r} (-1)^i \, Tr(f_i^m),$$

et par conséquent

$$\log Z(V;t) = \sum_{i=0}^{2r} (-1)^i \sum_{m \geqslant 1} Tr(f_i^m) \, t^m/m . \tag{4.3.5}$$

Mais K étant de caractéristique 0, on a, dans $K[[t]]$,

$$\det(1 - tf_i) = \exp\Big(-\sum_{m \geqslant 1} Tr(f_i^m) \, t^m/m\Big) \tag{4.3.6}$$

(c'est un résultat qui a déjà été mentionné au § 2, et qu'on peut prouver en triangularisant f_i sur la clôture algébrique $\overline{K}$ de K); si alors on pose $P_i^*(t) = \det(1 - tf_i)$, (4.3.5) et (4.3.6) donnent

$$Z(V;t) = \frac{P_1^*(t) \, P_3^*(t) \ldots P_{2r-1}^*(t)}{P_0^*(t) \, P_2^*(t) \ldots P_{2r}^*(t)}; \tag{4.3.7}$$

ceci prouve (CW1), moins le caractère algébrique des α_{ji}; mais il suffit de mettre le second membre de (4.3.7) sous forme irréductible, de noter $P_i(t)$ « ce qui reste » de $P_i^*(t)$ après cette simplification, et d'utiliser le théorème 2 et son corollaire 1, pour démontrer la totalité de (CW1).

Les conjectures (CW2) et (CW5) se démontrent de même à partir de (4.3.3) et (4.3.4). A l'heure actuelle, en revanche, les conjectures (CW3) et (CW4) ne semblent pas avoir été démontrées en toute généralité. Notons qu'il résulte de (CW3) que les polynômes de Weil P_i ne dépendent que de k

et V, et non du procédé, cohomologique ou autre, utilisé pour établir la formule (4.1.1).

§ 5. *Calcul explicite de certaines fonctions zêta.*

5.1. Ce dernier paragraphe donne, à titre d'illustration de ce qui précède, le calcul explicite des fonctions zêta de certaines variétés algébriques (courbes ou hypersurfaces) définies par des équations diagonales. On utilise essentiellement les résultats du chapitre 5, du chapitre 6 (§ 3), et le théorème suivant, dû à Davenport et Hasse (1934), qui permet de comparer les sommes de Gauss relatives à k et celles relatives à k_m ($m \geqslant 1$):

THÉORÈME 4 (Davenport-Hasse). — *Soient β et χ un caractère additif et un caractère multiplicatif non triviaux de k; pour $m \geqslant 1$, soient d'autre part $T^{(m)}$ et $N^{(m)}$ la trace et la norme dans l'extension k_m/k, et posons $\beta^{(m)} = \beta \circ T^{(m)}$, $\chi^{(m)} = \chi \circ N^{(m)}$. Alors*

(i) *$\beta^{(m)}$ est un caractère additif non trivial de k_m; $\chi^{(m)}$ est un caractère multiplicatif non trivial de k_m, et $\chi^{(m)}$ a même ordre que χ.*

(ii) *Si on désigne par τ et $\tau^{(m)}$ les sommes de Gauss $\tau(\chi \mid \beta)$ et $\tau(\chi^{(m)} \mid \beta^{(m)})$ relatives à k et k_m respectivement, on a*

$$\tau^{(m)} = (-1)^{m-1} \tau^m . \tag{5.1.1}$$

Démonstration. — (i) Il suffit de noter que $T^{(m)}: k_m^+ \to k^+$, et $N^{(m)}: k_m^* \to k^*$, sont des homomorphismes surjectifs (chap. 1, prop. 9 et 10).

(ii) (D'après Weil (1949), pp. 503-505). Pour tout polynôme unitaire $P(U) = U^h + a_1 U^{h-1} + \ldots + a_h$ appartenant à $k[U]$ (resp. à $k_m[U]$), posons $\varphi(P) = \beta(a_1)\chi(a_h)$ (resp. $\varphi^{(m)}(P) = \beta^{(m)}(a_1)\chi^{(m)}(a_h)$); φ et $\varphi^{(m)}$ sont évidemment des caractères multiplicatifs sur les anneaux principaux $k[U]$ et $k_m[U]$, et on peut leur associer, « à la Dirichlet », les « séries L » suivantes:

$$L(t) = \sum_{\substack{P \\ \text{unit.}}} \varphi(P)\, t^{\deg(P)} = \prod_{\substack{P \text{ unit.} \\ \text{irréd.}}} 1/(1 - \varphi(P)\, t^{\deg(P)}),$$

$$L_m(t) = \sum_{\substack{P \\ \text{unit.}}} \varphi^{(m)}(P)\, t^{\deg(P)} = \prod_{\substack{P \text{ unit.} \\ \text{irréd.}}} 1/(1 - \varphi^{(m)}(P)\, t^{\deg(P)}),$$

(P étant supposé appartenir à $k[U]$ et $k_m[U]$ respectivement, bien entendu.)

LEMME 1. — *On a* $L(t) = 1 + \tau t$, $L_m(t) = 1 + \tau^{(m)} t$.

Vérifions par exemple la première égalité. On a $L(t) = 1 + c_1 t + \ldots + c_h t^h + \ldots$, avec $c_h = \sum \varphi(P)$, cette somme étant étendue à tous les $P \in k[U]$ unitaires et de degré h, donc de la forme $U^h + a_1 U^{h-1} + \ldots + a_n$, les $a_i \in k$; pour $h = 1$, on trouve ainsi $c_1 = \sum_{a_1 \in k} \beta(a_1)\chi(a_1) = \tau$ (noter que $\bar{\chi}(0) = 0$); pour $h \geqslant 2$ au contraire, on trouve

$$c_h = q^{h-2}\Big(\sum_{a_1 \in k} \beta(a_1)\Big)\Big(\sum_{a_h \in k} \chi(a_h)\Big),$$

donc $c_h = 0$, chacune des deux sommes étant nulle (chap. 5, prop. 2 et 5).

LEMME 2. — *Si ω désigne une racine primitive m-ième de l'unité dans* **C**, *on a*

$$L_m(t^m) = \prod_{j=0}^{m-1} L(\omega^j t). \tag{5.1.2}$$

Pour chaque $P \in k[U]$, irréductible et unitaire, considérons le produit *fini*

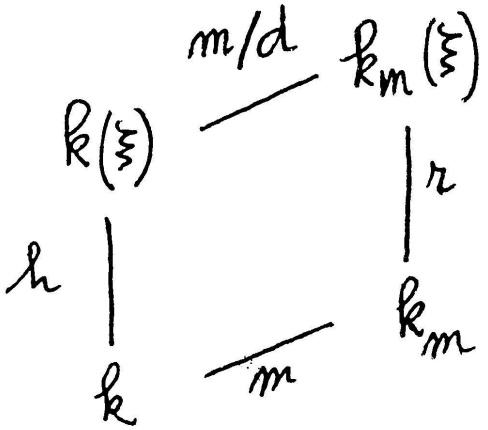
$$L_{m,P}(t^m) = \prod_{Q} 1/(1 - \varphi^{(m)}(Q)\, t^m),$$

Q parcourant seulement l'ensemble des facteurs irréductibles et unitaires de P dans $k_m[U]$; on a évidemment

$$L_m(t^m) = \prod_{\substack{P \text{ unit.} \\ \text{irréd.}}} L_{m,P}(t^m). \tag{5.1.3}$$

Transformons maintenant $L_{m,P}(t^m)$, P étant supposé fixé. Posons $h = \deg(P)$, et soit ξ une racine de P dans k; on a $[k(\xi):k] = h$, et bien entendu $[k_m:k] = m$; si alors $d = (h, m)$, le p.p.c.m. de h et m est égal à hm/d, et on a (chap. 1, prop. 4, cor. 1) $[k_m(\xi):k] = hm/d$, donc $[k_m(\xi):k_m] = h/d$. Il en résulte que la décomposition de P en facteurs irréductibles et unitaires de P dans $k_m[U]$ est de la forme

$$P = Q_1 Q_2 \ldots Q_d,$$



chacun des facteurs Q_i étant de degré $r = h/d$. Soit alors Q celui des Q_i dont ξ est racine, et calculons $\varphi^{(m)}(Q)$. Notons a_1 et a_n la trace et la norme de $-\xi$ dans l'extension $k(\xi)/k$, et b_1 et b_r la trace et la norme de $-\xi$ dans l'extension $k_m(\xi)/k_m$; on a $P(U) = U^h + a_1 U^{h-1} + \ldots + a_h$ et $Q(U) = U^r + b_1 U^{r-1} + \ldots + b_r$, et par conséquent

(5.1.4) $\varphi(P) = \beta(a_1)\,\chi(a_h)\,, \quad \varphi^{(m)}(Q) = \beta^{(m)}(b_1)\,\chi^{(m)}(b_r)\,.$

L'utilisation de la transitivité de la trace et de la norme dans le diagramme de corps ci-dessus donne d'autre part

(5.1.5) $T^{(m)}(b_1) = (m/d)\,a_1\,, \quad N^{(m)}(b_r) = a_h^{m/d}\,.$

(5.1.4), (5.1.5) et la définition de $\varphi^{(m)}$ permettent alors d'écrire

(5.1.6) $\varphi^{(m)}(Q) = \beta\big((m/d)\,a_1\big)\,\chi(a_h^{m/d}) = \varphi(P)^{m/d}\,.$

Les d facteurs irréductibles Q_i de P dans $k_m[U]$ donnent donc la même valeur à $\varphi^{(m)}$, d'où

(5.1.7) $L_{m,P}(t^m) = 1/(1-\varphi(P)^{m/d}t^{mh/d})^d\,.$

Mais, quel que soit $\alpha \in \mathbf{C}$, on a

(5.1.8) $(1-\alpha^{m/d}t^{mh/d})^d = \prod_{j=0}^{m-1}(1-\alpha(\omega^j t)^h)\,;$

les deux membres sont en effet des polynômes unitaires en t, à coefficients complexes, de même degré mh, et ayant les mêmes racines (toutes multiples d'ordre d). Dans (5.1.8), faisons $\alpha = \varphi(P)$, et portons dans (5.1.7); comme $h = \deg(P)$, il vient $L_{m,P}(t^m) = \prod_{j=0}^{m-1} 1/1(-\varphi(P)(\omega^j t)^{\deg(P)})$, ce qui, compte tenu de (5.1.3) et de la définition de $L(t)$, donne (5.1.2) et prouve le lemme 2.

Démontrons alors le théorème 4. Les lemmes 1 et 2 permettent d'écrire

$$1 + \tau^{(m)}t^m = \prod_{j=0}^{m-1}(1+\tau\omega^j t)\,;$$

la comparaison des termes de plus haut degré en t donne donc

$$\tau^{(m)} = \prod_{j=0}^{m-1}\tau\omega^j = \omega^{m(m-1)/2}\tau^m = (-1)^{m-1}\tau^m\,,$$

C.Q.F.D.

COROLLAIRE 1. — *Soient χ et ψ deux caractères multiplicatifs non triviaux de k, et supposons également $\chi\psi$ non trivial. Alors, si $\chi^{(m)} = \chi \circ N^{(m)}$ et si $\psi^{(m)} = \psi \circ N^{(m)}$, on a*

(5.1.9) $\pi(\chi^{(m)}, \psi^{(m)}) = (-1)^{m-1}\,\pi(\chi,\psi)^m\,.$

Démonstration. — Il suffit d'appliquer le théorème 4 et la proposition 9, (ii) du chapitre 5.

5.2. Appliquons alors le théorème 4 et son corollaire 1 au calcul des fonctions zêta des courbes de genre 1 étudiées au chapitre 6, sections 3.3 à 3.5 (dont on conserve les notations).

(1) *La courbe V_1 d'équation $Y^2 = 1 - X^3$ ($p \neq 2, 3$).*

Supposons d'abord $q \equiv 1 \pmod 6$; la formule (3.3.1) (chap. 6) appliquée au corps de base k_m donne $N_{1,m}^{\mathrm{aff}} = q^m + \pi(\varphi^{(m)}, \chi^{(m)}) + \pi(\varphi^{(m)}, \bar{\chi}^{(m)})$ $N_{1,m}^{\mathrm{aff}}$ étant évidemment le nombre de points de V_1 « à distance finie » et rationnels sur k_m; posons $\alpha = -\pi(\varphi, \chi)$, utilisons le corollaire 1 du théorème 4, et remarquons que V_1 admet exactement un point à l'infini, rationnel sur k; il vient alors $N_{1,m} = q^m + 1 - \alpha^m - \bar{\alpha}^m$, d'où finalement (th. 2, cor. 1):

$$Z(V_1; t) = (1-\alpha t)(1-\bar{\alpha}t)/(1-t)(1-qt), \tag{5.2.1}$$

ce qui est évidemment conforme au théorème 3.

Supposons maintenant $q \equiv -1 \pmod 6$ (donc $p \equiv -1 \pmod 6$ et f impair). On aura besoin du lemme suivant:

LEMME 1. — *Soit $p \equiv -1 \pmod 6$, et soient φ_2 et χ_2 deux caractères multiplicatifs de $K = \mathbf{F}_{p^2}$, respectivement d'ordre 2 et d'ordre 3 (noter que $p^2 \equiv 1 \pmod 6$). Alors $\pi(\varphi_2, \chi_2) = p$.*

Démonstration. — Comme K contient six racines 6-ièmes de l'unité, il est facile de voir que le nombre N de solutions dans K^2 de l'équation $Y^2 = 1 - X^3$ satisfait à $N \equiv 5 \pmod 6$ (comparer avec le chap. 6, sect. A.1, exemple 2). Posons $\pi = \pi(\varphi_2, \chi_2)$; on a $N = p^2 + \pi + \bar{\pi}$ (chap. 6, (3.3.1)), et la congruence relative à N donne

$$\pi + \bar{\pi} \equiv 4 \pmod 6. \tag{5.2.2}$$

Mais $\pi, \bar{\pi} \in \mathbf{Z}[\rho]$ ($\rho = e^{2\pi i/3}$), $\pi\bar{\pi} = p^2$ (chap. 5, prop. 9, cor. 1), et p est *inerte* dans $\mathbf{Z}[\rho]$; ainsi, $\pi = \varepsilon p$, $\bar{\pi} = \bar{\varepsilon} p$, ε étant une racine 6-ième de l'unité. (5.2.2) donne alors $(\varepsilon + \bar{\varepsilon})p \equiv 4 \pmod 6$, puis $\varepsilon + \bar{\varepsilon} \equiv -4 \equiv 2 \pmod 6$, ce qui implique $\varepsilon = 1$ (examiner les six valeurs possibles de ε). Finalement, $\pi = \varepsilon p = p$, C.Q.F.D.

Calculons alors $N_{1,m}^{\mathrm{aff}}$. Si m est impair, on a $q^m \equiv -1 \pmod 3$, donc $N_{1,m}^{\mathrm{aff}} = q^m$. Supposons maintenant m pair, $m = 2m'$, et soient φ et χ deux caractères multiplicatifs de k_2, respectivement d'ordre 2 et d'ordre 3; le lemme 1 et le corollaire 1 du théorème 4 (appliqué à $k_2/\mathbf{F}_{p^2}$) donnent d'abord $\pi(\varphi, \chi) = (-1)^{f-1}p^f = q$; le corollaire 1 du théorème 4, appliqué à k_m/k_2, donne d'autre part $\pi(\varphi^{(m')}, \chi^{(m')}) = (-1)^{m'-1}q^{m'} = -(-q)^{m'}$,

donc (chap. 6, (3.3.1)) $N_{1,m}^{\mathrm{aff}} = q^m - 2(-q)^{m/2}$. Posons alors $\alpha = iq^{1/2}$; les calculs précédents montrent que, quelle que soit la parité de m, on a $N_{1,m}^{\mathrm{aff}} = q^m - \alpha^m - \bar{\alpha}^m$, donc $N_{1,m} = q^m + 1 - \alpha^m - \bar{\alpha}^m$; finalement, on trouve encore

$$Z(V_1; t) = (1-\alpha t)(1-\bar{\alpha}t)/(1-t)(1-qt); \tag{5.2.3}$$

compte tenu de la valeur explicite $\alpha = iq^{1/2}$, on a même, dans ce cas,

$$Z(V_1; t) = (1+qt^2)/(1-t)(1-qt). \tag{5.2.4}$$

(2) *La courbe V_2 d'équation $Y^2 = 1 - X^4$ ($p \neq 2$).*

Supposons d'abord $q \equiv 1 \pmod 4$; la formule (3.3.2) (chap. 6) appliquée au corps de base k_m, combinée au corollaire 1 du théorème 4, donne, comme en (1), $N_{2,m}^{\mathrm{aff}} = q^m - 1 - \alpha^m - \bar{\alpha}^m$, avec $\alpha = -\pi(\varphi, \psi)$; d'autre part, V_2 admet à l'infini un point double rationnel sur k: comptons-le pour *deux* (ce qui revient à remplacer V_2 par sa normalisée V_2^* : voir d'ailleurs chap. 8, sect. 2.4); on trouve ainsi $N_{2,m}^* = q^m + 1 - \alpha^m - \bar{\alpha}^m$, donc

$$Z(V_2^*; t) = (1-\alpha t)(1-\bar{\alpha}t)/(1-t)(1-qt), \tag{5.2.5}$$

ce qui est toujours conforme au théorème 3. Remarquer que la fonction zêta de V_2 *non normalisée* est $Z(V_2; t) = (1-\alpha t)(1-\bar{\alpha}t)/(1-qt)$.

Si on suppose au contraire $q \equiv -1 \pmod 4$, un calcul analogue à celui fait en (1) (pour $q \equiv -1 \pmod 6$) donnerait encore

$$Z(V_2^*; t) = (1+qt^2)/(1-t)(1-qt). \tag{5.2.6}$$

(3) *La courbe V_3 d'équation $Y^3 = 1 - X^3$ ($p \neq 3$).*

On laisse au lecteur le soin de vérifier que les formules (5.2.5) et (5.2.6) restent valides pour la normalisée V_3^* de V_3, respectivement pour $q \equiv 1 \pmod 3$ (et avec $\alpha = -\pi(\chi, \chi)$: voir chap. 6, (3.3.3)), d'une part; et pour $q \equiv -1 \pmod 3$, d'autre part.

(4) *La courbe V_4 d'équation $Y^2 = X - X^3$* (pour $q \equiv 1 \pmod 4$).

Il résulte des calculs faits au chapitre 6 (sect. 3.4) que

$$Z(V_4; t) = Z(V_2^*; t). \tag{5.2.7}$$

(En fait, V_4 est un modèle projectif non singulier de V_2, de sorte qu'on peut choisir pour V_2^* la courbe V_4.) L'égalité (5.2.7) reste d'ailleurs vraie pour $q \equiv -1 \pmod 4$.

5.3. Terminons par deux exemples simples d'hypersurfaces (dans $\mathbf{P}_3$).

(5) *La quadrique d'équation homogène* $X^2 + Y^2 + Z^2 + T^2 = 0$ $(p \neq 2)$.

Le nombre $N_m{}^c$ de points rationnels sur k_m du *cône* défini dans $\mathbf{A}_4$ par l'équation ci-dessus est donné (chap. 6, th. 1) par

$$N_m{}^c = q^{3m} + q^{-m}(q^m - 1)\,\tau(\varphi^{(m)})^4\,,$$

φ désignant le caractère de Legendre de k; mais $\tau(\varphi^{(m)})^2 = q^m\,\varphi^{(m)}(-1)$, et $(q^m - 1)\,N_m + 1 = N_m{}^c$ (N_m étant le nombre de points de la quadrique rationnels sur k_m); d'où immédiatement $N_m = q^{2m} + 2q^m + 1$, et (th. 2, cor. 1)

$$Z(V_5; t) = 1/(1-t)\,(1-qt)^2\,(1-q^2t)\,, \tag{5.3.1}$$

V_5 désignant la quadrique étudiée. (On aurait pu calculer $N_m{}^c$ à l'aide des formules du chap. 6, prop. 2). Ce résultat est évidemment conforme à (4.2.1) (sect. 4.2), c'est-à-dire au théorème de Dwork pour les hypersurfaces: on a $P(t) = 1 - qt$, de degré 1, et $(-1)^n = (-1)^3 = -1$, ce qui « envoie » $P(t)$ au dénominateur.

(6) *La surface cubique d'équation homogène* $X^3 + Y^3 + Z^3 + T^3 = 0$ $(p \neq 3)$.

On se limitera pour simplifier au cas où $q \equiv 1 \pmod 3$. On pourrait procéder comme en (5), et utiliser le théorème 1 du chapitre 6. Il est plus commode de remarquer que (avec des notations évidentes) $N_m = N_m^{\mathrm{aff}} + N_m^{\mathrm{inf}}$; N_m^{aff} est le nombre de solutions rationnelles sur k_m de l'équation $X^3 + Y^3 + Z^3 = -1$; si χ est un caractère multiplicatif d'ordre 3 de k, le théorème 2 du chapitre 6, la proposition 10 du chapitre 5 et le théorème 4 ci-dessus donnent

$$N_m^{\mathrm{aff}} = q^{2m} + (-\pi_1)^m + (-\bar{\pi}_1)^m + 3\,\pi_2{}^m + 3\,\bar{\pi}_2{}^m\,, \tag{5.3.2}$$

avec $\pi_1 = \pi(\chi, \chi) = -\pi(\chi, \chi, \chi)$ (chap. 5, prop. 10, (i)) et $\pi_2 = \pi(\chi, \chi, \bar{\chi})$; quant à N_m^{inf}, c'est le nombre de points rationnels sur k_m de la cubique d'équation projective $X^3 + Y^3 + Z^3 = 0$; d'où

$$N_m^{\mathrm{inf}} = q^m + 1 - (-\pi_1)^m - (-\pi_1)^m \tag{5.3.3}$$

(chap. 6, (3.3.3); tenir compte des trois points à l'infini !): au total,

$$N_m = q^{2m} + q^m + 1 + 3\,\pi_2{}^m + 3\,\bar{\pi}_2{}^m\,, \tag{5.3.4}$$

et (th. 2, cor. 1, une dernière fois)

(5.3.5) $\quad Z(V_6; t) = 1/(1-t)(1-qt)(1-q^2t)(1-\pi_2 t)^3(1-\bar{\pi}_2 t)^3$,

V_6 désignant la surface cubique étudiée. Ce résultat est conforme aux conjectures de Weil: on a $P_0(t) = 1 - t$, $P_1(t) = P_3(t) = 1$, $P_4(t) = 1 - q^2t$, et $P_2(t) = (1-qt)(1-\pi_2 t)^3(1-\pi_2 t)^3$; l'hypothèse de Riemann se réduit à $|\pi_2| = |\bar{\pi}_2| = |\pi(\chi, \chi, \bar{\chi})| = q$ (chap. 5, prop. 10, cor. 1, (ii)); la « caractéristique d'Euler-Poincaré » est égale à $1 + 7 + 1 = 9$, et l'équation fonctionnelle s'écrit $Z(V_6; 1/q^2t) = -q^9t^9Z(V_6; t)$.

Notes sur le chapitre 9

§ **1-2-3-4**: l'idée d'étudier arithmétiquement un corps de fonctions algébriques d'une variable sur un corps fini semble apparaître nettement pour la première fois chez Dedekind (1857). Mais c'est dans la thèse d'Artin (1924), puis dans les travaux de Schmidt (1931) et Hasse (1933, 1934, 1936), qu'est définie la notion de fonction zêta (« Kongruenzzetafunktion ») et formulée l'« hypothèse de Riemann » en caractéristique p (Artin, Schmidt, Hasse utilisent le langage des corps de fonctions algébriques d'une variable, et non celui des courbes: mais ces deux langages sont équivalents, ou plutôt, le sont devenus depuis les « Foundations » de Weil; voir d'ailleurs Weil (1949), *Introduction*). L'équation fonctionnelle pour $\zeta(V; s)$ (c'est-à-dire, aux notations près, la proposition 3) est due à Schmidt (1931); la démonstration de l'hypothèse de Riemann pour $g = 1$ est due à Hasse (1933, 1934), et, pour g quelconque, à Weil (1940; 1948, a). Les diverses définitions de $Z(V; t)$ données au paragraphe 1 figurent, pour une courbe, dans Weil (1948, a), et, pour une variété projective non singulière de dimension quelconque, dans Weil (1949); cet article contient également l'énoncé (et, pour des cas particuliers, la vérification) des « conjectures de Weil ». L'existence d'une « formule de Lefschetz » en géométrie algébrique est conjecturée dans Weil (1954) (p. 556): d'où la notion de « cohomologie de Weil » — cette terminologie étant d'ailleurs considérée par Weil lui-même comme « tout à fait inadéquate » (*wholly unsuitable*). Au sujet du lien formel entre théories cohomologiques des variétés algébriques et propriétés des fonctions zêta, voir Demazure (1969), notamment §§ 7 et 9. Au sujet du lien entre méthodes p-adiques et méthodes cohomologiques, voir Katz (1972) (cet exposé contient une abondante bibliographie).

Signalons qu'à côté des fonctions zêta, on peut (comme en arithmétique) construire, pour les variétés algébriques, des « séries L »; pour une définition générale (en langage des schémas, et englobant d'ailleurs les séries L de la théorie des nombres), voir [**16**], pp. 86-91. La rationalité des séries L des

variétés algébriques a été établie par Grothendieck (1964, b); voir également Dwork (1966, b). Pour l'application de ce résultat à l'étude des sommes exponentielles, voir notamment Bombieri (1966).

§ **5**: les exemples de ce paragraphe sont empruntés essentiellement à Davenport-Hasse (1934) et à Weil (1949). Signalons que le lemme 1 (sect. 5.2) peut aussi se démontrer à l'aide de la proposition 9, (ii) (chap. 5), et du résultat suivant, dû à Stickelberger (1890): si χ est un caractère multiplicatif de $\mathbf{F}_{p^2}$, et si θ est un élément primitif de $\mathbf{F}_{p^2}/\mathbf{F}_p$, on a $\tau(\chi \mid \beta) = \chi(\theta)\, p$, si $p \neq 2$, et $\tau(\chi \mid \beta) = p$ si $p = 2$; pour une démonstration de ce dernier énoncé, voir aussi Carlitz (1956, a).

Pour $V = V_1$ et $q \equiv -1 \pmod 6$, ou $V = V_2{}^*$ et $q \equiv -1 \pmod 4$, ou $V = V_3{}^*$ et $q \equiv -1 \pmod 3$, on a trouvé la même expression

$$Z(V; t) = (1+qt^2)/(1-t)\,(1-qt);$$

ceci résulte (1) du fait que, dans les trois cas, on a $N_1 = q + 1$, et (2) de la relation $Z(V; t) = (1 + (N_1 - q - 1)\, t + qt^2)/(1-t)\,(1-qt)$, valable pour toute courbe V (projective, non singulière) de genre 1, définie sur k et ayant N_1 points rationnels sur k (cette relation se déduit facilement du théorème 3 et du théorème 2, corollaire 1 et remarque). En fait, si deux courbes de genre 1, définies sur k, ont même nombre N_1 de points rationnels sur k, alors, elles ont le même nombre N_m de points rationnels sur k_m pour tout m, puisqu'elles ont même fonction zêta (appliquer la formule ci-dessus !): on peut prouver que ceci se produit si et seulement si les deux courbes sont isogènes sur k (voir [**4**], p. 242, pour la partie « si », et Tate (1966), pour la partie « seulement si ».)

BIBLIOGRAPHIE

1. *Ouvrages généraux, monographies.*

[1] Artin, E. *Geometric Algebra*, Interscience Publishers (1957).

[2] —— *Algebraic Numbers and Algebraic Functions*, Gordon and Breach (1967).

[3] Borevich, Z. I. and I. R. Shafarevich. *Number Theory*, Academic Press (1966).

[4] Cassels, J. W. S. *Diophantine equations with special reference to elliptic curves* (survey article), J. London Math. Soc., 41 (1966), pp. 193-291.

[5] Eichler, M. *Introduction to the theory of algebraic numbers and functions*, Academic Press (1966).

[6] Gel'fand, A. et I. Linnik. *Méthodes élémentaires dans la théorie analytique des nombres*, Gauthier-Villars (1965).

[7] Greenberg, M. J. *Lectures on forms in many variables*, Benjamin (1969).