Zeitschrift: L'Enseignement Mathématique
Band: 19 (1973)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI
Kapitel: §5. Calcul explicite de certaines fonctions zêta.
Autor: Joly, Jean-René
DOI: https://doi.org/10.5169/seals-46287

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*

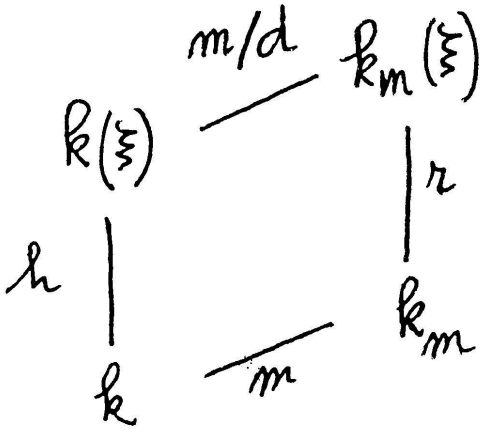
$$L_{m,P}(t^m) = \prod_{Q} 1/(1 - \varphi^{(m)}(Q)\, t^m),$$

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