

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

**Artikel:** ÉQUATIONS ET VARIÉTÉS ALGÈBRIQUES SUR UN CORPS FINI  
**Autor:** Joly, Jean-René  
**Kapitel:** §4. Conjectures de Weil.  
**DOI:** <https://doi.org/10.5169/seals-46287>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

**Download PDF:** 20.02.2025

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

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'analogie 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  $\alpha_i$  ( $1 \leq i \leq 2g$ ) les inverses des  $2g$  zéros de  $P(t)$ ; on a alors  $Z(V; t) = (1-\alpha_1 t) \dots (1-\alpha_{2g} t)/(1-t)(1-qt)$ , donc (voir sect. 2.2),  $N_m = q^m + 1 - \alpha_1^m - \dots - \alpha_{2g}^m$ ; pour  $m = 1$ , ceci permet d'écrire  $|q + 1 - N_1| \leq |\alpha_1| + \dots + |\alpha_{2g}|$ ; si maintenant on suppose que les  $2g$  zéros de  $P$  ont pour module  $q^{-1/2}$ , on a  $|\alpha_i| = q^{1/2}$  pour  $i = 1, \dots, 2g$ , et la dernière inégalité se réduit (puisque  $N = N_1$ ) à

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

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  $\zeta$  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  $(\alpha_{ji})_{1 \leq j \leq B_i}$ ,  $0 \leq i \leq 2r$ , telles qu'en posant, pour chaque  $i$ ,*

$$P_i(t) = \prod_{j=1}^{B_i} (1 - \alpha_{ji}t), \text{ on ait}$$

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

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

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

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

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

$$(4.1.3) \quad |\alpha_{ji}| = q^{i/2}.$$

(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  $\mathfrak{D}$ , contenu dans  $\mathbb{C}$ , et dont le corps résiduel s'identifie à  $k$ , et une variété projective non singulière  $V_0$ , définie sur  $\mathfrak{D}$ , et dont la variété réduite modulo l'idéal maximal de  $\mathfrak{D}$  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  $\chi$ , 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

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

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

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

$P(t)$  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  $i \geq 0$ , 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  $V \rightarrow V$ , 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  $\Gamma$  de  $f$  avec la diagonale  $\Delta$  de  $V \times V$  est donné par*

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

(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  $0 \leq i \leq 2r$  une application bilinéaire  $H^i(V) \times H^{2r-i}(V) \rightarrow H^{2r}(V) \simeq K$  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  $\Gamma$  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

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

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

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

et par conséquent

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

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

$$(4.3.6) \quad \det(1 - tf_i) = \exp\left(-\sum_{m \geq 1} \operatorname{Tr}(f_i^m) t^m / m\right)$$

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

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

ceci prouve (CW1), moins le caractère algébrique des  $\alpha_{ji}$ ; 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  $k_m$  ( $m \geq 1$ ):

THÉORÈME 4 (Davenport-Hasse). — *Soient  $\beta$  et  $\chi$  un caractère additif et un caractère multiplicatif non triviaux de  $k$ ; pour  $m \geq 1$ , 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  $\chi$ .

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

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

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

(ii) (D'après Weil (1949), pp. 503-505). Pour tout polynôme unitaire  $P(U) = U^h + a_1 U^{h-1} + \dots + a_h$  appartenant à  $k[U]$  (resp. à  $k_m[U]$ ), posons  $\varphi(P) = \beta(a_1) \chi(a_h)$  (resp.  $\varphi^{(m)}(P) = \beta^{(m)}(a_1) \chi^{(m)}(a_h)$ );  $\varphi$  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.)