# 1. On Zeta-Functions and L-Series of Algebraic Varieties

By Makoto ISHIDA
Mathematical Institute, University of Tokyo
(Comm. by Z. SUETUNA, M.J.A., Jan. 13, 1958)

In this paper, we shall prove Weil's conjecture on zeta-functions for algebraic varieties, defined over finite fields, having abelian varieties as abelian (not necessarily unramified) coverings and also Lang's analogous conjecture on $L$-series for those coverings. Then we shall see some interesting relation between the zeta-functions of such algebraic varieties and those of their Albanese varieties. Moreover those results will enable us to prove Hasse's conjecture on zeta-functions for some algebraic varieties defined over algebraic number fields. In the following we shall use the definitions, notations and results of Weil's book [6] often without references.

Here I wish to express my hearty gratitude to Prof. Z. Suetuna for his encouragement and also to Mr. Y. Taniyama for his kind suggestions.

1. Let $V$ be a normal projective variety of dimension $r$, defined over a finite field $k$ with $q$ elements; let $A$ be an abelian variety such that $f: A\rightarrow V$ is a Galois (not necessarily unramified) covering, also defined over $k$, with group $G$ and of degree $n$ (cf. Lang [2]). The map $a\rightarrow a^q$ for all points $a$ on $A$ determines an endomorphism of $A$, which is denoted by $\pi=\pi_A$. Let $x$ be a generic point of $A$ over $k$. Then, for $\sigma$ in $G$, the map $x\rightarrow x^\sigma$ induces a birational transformation of $A$ defined over $k$; hence we can write $x^\sigma=\eta_\sigma(x)+a_\sigma$ where $\eta_\sigma$ is an automorphism of $A$ defined over $k$ and $a_\sigma$ is a rational point on $A$ over $k$.

Now we consider an endomorphism $\pi^m-\eta_\sigma$ of $A$ for a positive rational integer $m$ and for $\sigma$ in $G$. As $k(\eta_\sigma(x))=k(x)$, we have $k(x^{q^m}, (\pi^m-\eta_\sigma)(x))=k(x)$ and so $\nu_i(\pi^m-\eta_\sigma)=1$. Hence the order of the kernel of this endomorphism is equal to $\det M_l(\pi^m-\eta_\sigma)$, with a rational prime $l$ different from the characteristic of $k$, which is denoted by $\nu(m,\sigma)$. As $\det M_l(\eta_\sigma)=1$ and the matrix $M_l(\pi^m\eta_\sigma^{-1}-1)$ is of even degree $2r$, we have also $\nu(m,\sigma)=\det M_l(1-\pi^m\eta_\sigma^{-1})$.

Then the $L$-series $L(u,\chi,A/V)$ of the covering $A/V$ belonging to an irreducible character $\chi$ of $G$ is given by the following logarithmic derivative:

$$d/du\cdot\log L(u,\chi,A/V)=\sum_{m=1}^{\infty}\{1/n\cdot\sum_{\sigma\in G}\chi(\sigma)\nu(m,\sigma)\}u^{m-1}$$

**Theorem 1.** *Let $Z(u,V)$ and $Z(u,A)$ be the zeta-functions of $V$ and $A$ over $k$. Then we have the equality $Z(u,V)=Z(u,A)$ if and* *only if $V$ is also an abelian variety defined over $k$. When that is so, $G$ is abelian and $A/V$ is unramified and, moreover, all the L-series $L(u,\chi,A/V)$ with $\chi$ different from the principal character $\chi_0$ are trivially equal to* 1.

Proof. Generally we have

$$d/du\cdot\{n\cdot\log(Z(u,A)/Z(u,V))\}=\textstyle\sum_{m=1}^{\infty}\{n\cdot\nu(m,1)-\sum_{\sigma\in G}\nu(m,\sigma)\}u^{m-1}.$$

We divide the sum $\sum_\sigma$ in the right side of this equality as follows:

$$\textstyle\sum_\sigma=\sum_{Z_j}\sum_{\sigma_{j,i}},$$

where $Z_j$ ranges over all the cyclic subgroups of $G$ (not excluding $Z=\{1\}$) and $\sigma_{j,i}$ ranges over all the generators of $Z_j$. For each fixed $j$, we can transform all the matrices $M_l(\eta_{\sigma_{j,i}})$ and $M_l(\pi)$ into diagonal forms simultaneously:

$$M_l(\eta_{\sigma_{j,i}})=\begin{pmatrix}\ddots & & 0\\ & \zeta_{j,i,\mu} & \\ 0 & & \ddots\end{pmatrix},\quad M_l(\pi)=\begin{pmatrix}\ddots & & 0\\ & \pi_\mu & \\ 0 & & \ddots\end{pmatrix}.$$

Here we note that all $\zeta_{j,i,\mu}$ are some roots of unity and, for each fixed $j$ and $\mu$, all $\zeta_{j,i,\mu}$ are algebraically conjugate to each other. Then we have

$$\begin{aligned}&n\cdot\nu(m,1)-\textstyle\sum_\sigma\nu(m,\sigma)\\&\quad=\textstyle\sum_t\sum_{\mu_1,\dots,\mu_t}(-1)^t(n-\sum_{Z_j}\sum_{\sigma_{j,i}}\zeta_{j,i,\mu_1}^{-1}\cdots\zeta_{j,i,\mu_t}^{-1})(\pi_{\mu_1}\cdots\pi_{\mu_t})^m,\end{aligned}$$

and, by the above remark and by the equality $n=\sum_{Z_j}\sum_{\sigma_{j,i}}1$, $n_{\mu_1,\dots,\mu_t}=n-\sum_{Z_j}\sum_{\sigma_{j,i}}\zeta_{j,i,\mu_1}^{-1}\cdots\zeta_{j,i,\mu_t}^{-1}$ are non-negative rational integers. Hence we have

$$\begin{aligned}&d/du\cdot\{n\cdot\log(Z(u,A)/Z(u,V))\}\\&\quad=\textstyle\sum_{m=1}^{\infty}\sum_t\sum_{\mu_1,\dots,\mu_t}(-1)^t n_{\mu_1,\dots,\mu_t}(\pi_{\mu_1}\cdots\pi_{\mu_t})^m u^{m-1},\end{aligned}$$

and so

$$(Z(u,A)/Z(u,V))^n=\Pi_t\{\Pi_{\mu_1,\dots,\mu_t}(1-\pi_{\mu_1}\cdots\pi_{\mu_t}u)^{n_{\mu_1,\dots,\mu_t}}\}^{(-1)^{t+1}}.$$

Then as, by Taniyama [5], all the characteristic roots $\pi_\mu$ of $M_l(\pi)$ are of absolute values $q^{1/2}$, the equality $Z(u,V)=Z(u,A)$ implies that all $n_{\mu_1,\dots,\mu_t}=0$ and so all $\zeta_{j,i,\mu}=1$. Hence then all $\eta_\sigma$ are the identity automorphism of $A$ and so $A/V$ is unramified. Therefore the 'only if' part of our theorem is proved. As for the 'if' part, it is easily verified because $V$ is then isogenous to $A$ and $M_l(\pi_V)$ and $M_l(\pi_A)$ have the same characteristic roots.

2. **Theorem 2.** *If $G$ is abelian, then the zeta-function $Z(u,V)$ and the L-series $L(u,\chi,A/V)$ with $\chi\neq\chi_0$ are expressed as follows:*

$$Z(u,V)=P_1(u)P_3(u)\cdots P_{2r-1}(u)/P_0(u)P_2(u)\cdots P_{2r}(u),$$

$$L(u,\chi,A/V)=Q_1^{(\chi)}(u)Q_3^{(\chi)}(u)\cdots Q_{2r-1}^{(\chi)}(u)/Q_2^{(\chi)}(u)\cdots Q_{2r-2}^{(\chi)}(u),$$

*where $P_t(u)$ and $Q_t^{(\chi)}(u)$ are polynomials of $u$ such that*

$$P_t(u)=\Pi_j(1-\alpha_j^{(t)}u),\quad Q_t^{(\chi)}(u)=\Pi_j(1-\beta_j^{(t,\chi)}u)$$

*with $|\alpha_j^{(t)}|$, $|\beta_j^{(t,\chi)}|=q^{t/2}$. Especially $P_0(u)=1-u$ and $P_{2r}(u)=1-q^r u$. Moreover if we put $e=\sum_t(-1)^t deg\,P_t$ and $e(\chi)=\sum_t(-1)^t deg\,Q_t^{(\chi)}$, then we have functional equations:*

$$Z(1/q^r u, V)=(-1)^e q^{re/2} u^e Z(u, V),$$
$$L(1/q^r u, \chi, A/V)=(-1)^{e(\chi)} q^{re(\chi)/2} u^{e(\chi)} L(u, \overline{\chi}, A/V).$$

Proof. As $G$ is abelian and $\pi$ commutes with every $\eta_\sigma$, we can transform all the matrices $M_l(\eta_\sigma)$ and $M_l(\pi)$ into diagonal forms simultaneously:

$$M_l(\eta_\sigma)=\begin{pmatrix} \zeta_1^{(\sigma)} & & 0 \\ & \ddots & \\ 0 & & \zeta_{2r}^{(\sigma)} \end{pmatrix}, \quad M_l(\pi)=\begin{pmatrix} \pi_1 & & 0 \\ & \ddots & \\ 0 & & \pi_{2r} \end{pmatrix}.$$

Then the map $\sigma\to\zeta_j^{(\sigma)}$ is an irreducible character of $G$, which is denoted by $\lambda_j$; and we have $\nu(m,\sigma)=\det M_l(1-\pi^m\eta_\sigma^{-1})=\Pi_\mu(1-\pi_\mu^m\lambda_\mu^{-1}(\sigma))$ $=\sum_t\sum_{\mu_1,\cdots,\mu_t}(-1)^t(\pi_{\mu_1}\cdots\pi_{\mu_t})^m\lambda_{\mu_1}^{-1}\cdots\lambda_{\mu_t}^{-1}(\sigma)$. Hence we have, for any irreducible character $\chi$ of $G$ (not excluding the principal character $\chi_0$),

$$d/du\cdot\log L(u,\chi,A/V)=\textstyle\sum_{m=1}^\infty\sum_t(-1)^t\sum_{\mu_1,\cdots,\mu_t}(\pi_{\mu_1}\cdots\pi_{\mu_t})^m \times\{1/n\cdot\sum_{\sigma\in G}\chi(\sigma)\lambda_{\mu_1}^{-1}\cdots\lambda_{\mu_t}^{-1}(\sigma)\}u^{m-1};$$

and so, by the orthogonal relation of group-characters, we have

$$d/du\cdot\log L(u,\chi,A/V) =\textstyle\sum_{m=1}^\infty\sum_t(-1)^t\sum_{\mu_1,\cdots,\mu_t\,:\,\chi=\lambda_{\mu_1}\cdots\lambda_{\mu_t}}(\pi_{\mu_1}\cdots\pi_{\mu_t})^m u^{m-1}.$$

Thus we have

$$L(u,\chi,A/V)=\Pi_t\{\Pi_{\mu_1,\cdots,\mu_t\,:\,\chi=\lambda_{\mu_1}\cdots\lambda_{\mu_t}}(1-\pi_{\mu_1}\cdots\pi_{\mu_t}u)\}^{(-1)^{t+1}}.$$

As all $\pi_\mu$ are of absolute values $q^{1/2}$, our first statement is proved. As for functional equations, it suffices to note that $\pi_1\pi_2\cdots\pi_{2r}=\det M_l(\pi)$ $=q^r$ and $\lambda_1\lambda_2\cdots\lambda_{2r}(\sigma)=\det M_l(\eta_\sigma)=1=\chi_0(\sigma)$ for any $\sigma$ in $G$.

Remark. In the case where $G$ is not necessarily abelian, using the fundamental result of Artin on induced characters in [1] and Theorem 2, we can also prove that *the $n$-th powers of $Z(u, V)$ and $L(u,\chi,A/V)$ are polynomials of $u$ and their zeros and poles are of absolute values $q^{-t/2}$ with $0\leq t\leq 2r$.*

3. Now let $B$ be an abelian variety, defined over $k$, which is generated by $V$ and a rational map $\beta$ of $V$ into $B$ (cf. Matsusaka [3]). Then $\beta\circ f$ is a rational map of $A$ into $B$ and we may assume, without loss of generality, that $\lambda=\beta\circ f$ is a homomorphism of $A$ into $B$ and then it is easily verified that $\lambda$ is onto. As $a_\sigma=\eta_\sigma(0)+a_\sigma$, we have $f(a_\sigma)=f(0)$ and so $\lambda(a_\sigma)=\lambda(0)=0$ for any $\sigma$ in $G$. If $x$ is a generic point of $A$ over $k$, then we have $\lambda(x)=\lambda(x^\sigma)=\lambda(\eta_\sigma(x)+a_\sigma)=\lambda(\eta_\sigma(x))$ and so $\lambda((\eta_\sigma-1)(x))=0$. Thus the kernel of $\lambda$ must contain all the loci $C_\sigma$ of $(\eta_\sigma-1)(x)$ over $k$ for all $\sigma$ in $G$. (Clearly $C_\sigma$ is an abelian subvariety of $A$ defined over $k$.) Conversely if, for an abelian variety $B$ defined over $k$, there exists a homomorphism $\lambda$ of $A$ onto $B$ with kernel containing all $C_\sigma$, then there exists a rational map $\beta$ of $V$ onto $B$ such that $\lambda=\beta\circ f$.

Hence, by the characterization of Albanese varieties in Matsusaka [3], there exist an abelian variety $B$ defined over $k$, which is isogenous to the Albanese variety of $V$, and a homomorphism $\lambda$ of $A$ onto $B$, whose kernel is the smallest algebraic subgroup of $A$ containing all $C_\sigma$.

Let $G$ be abelian. Then for any $\sigma$, $\tau$ in $G$, we have $(\eta_\sigma-1)(\eta_\tau-1)=(\eta_\tau-1)(\eta_\sigma-1)$ and so $(\eta_\sigma-1)C_\tau$ is contained in $C_\tau$. Moreover, as $\dim(\eta_\sigma-1)C_\sigma=\dim(\eta_\sigma-1)^2A=1/2\cdot\mathrm{rank}\,M_l(\eta_\sigma-1)^2=1/2\cdot\mathrm{rank}\,M_l(\eta_\sigma-1)=\dim C_\sigma$, we have also $(\eta_\sigma-1)C_\sigma=C_\sigma$. If we denote the elements of $G$ by $\sigma_0=1, \sigma_1,\cdots,\sigma_{n-1}$, then the 0-component of the kernel of our homomorphism $\lambda$ is clearly the locus $C$ of $(\eta_{\sigma_1}-1)(x_1)+\cdots+(\eta_{\sigma_{n-1}}-1)(x_{n-1})$ over $k$ where $x_1,\cdots,x_{n-1}$ are independent generic points of $A$ over $k$; and then the dimension of $C$ is given by $\sum_i\dim C_{\sigma_i}-\sum_{i<j}\dim(C_{\sigma_i}\cap C_{\sigma_j})+\sum_{i<j<h}\dim(C_{\sigma_i}\cap C_{\sigma_j}\cap C_{\sigma_h})-\cdots$ . (Here conveniently we denote the dimension of a component of $C_{\sigma_{i_1}}\cap C_{\sigma_{i_2}}\cap\cdots\cap C_{\sigma_{i_t}}$ by $\dim(C_{\sigma_{i_1}}\cap C_{\sigma_{i_2}}\cap\cdots\cap C_{\sigma_{i_t}})$.) As $\eta_{\sigma_i}-1$ induces a homomorphism on the 0-component of $C_{\sigma_i}\cap C_{\sigma_j}$ with finite kernel, $\dim(C_{\sigma_i}\cap C_{\sigma_j})$ is equal to the dimension of its image under $\eta_{\sigma_i}-1$, which is contained in $(\eta_{\sigma_i}-1)(\eta_{\sigma_j}-1)A$ and so of dimension $\leq 1/2\,\mathrm{rank}\,M_l(\eta_{\sigma_i}-1)(\eta_{\sigma_j}-1)$. While, as $G$ is abelian, $(\eta_{\sigma_i}-1)(\eta_{\sigma_j}-1)A$ is contained in the 0-component of $C_{\sigma_i}\cap C_{\sigma_j}$. Hence we have $\dim(C_{\sigma_i}\cap C_{\sigma_j})=1/2\cdot\mathrm{rank}\,M_l(\eta_{\sigma_i}-1)(\eta_{\sigma_j}-1)$; and similarly $\dim(C_{\sigma_{i_1}}\cap C_{\sigma_{i_2}}\cap\cdots\cap C_{\sigma_{i_t}})=1/2\cdot\mathrm{rank}\,M_l(\eta_{\sigma_{i_1}}-1)(\eta_{\sigma_{i_2}}-1)\cdots(\eta_{\sigma_{i_t}}-1)$. Therefore $2\cdot\dim C$ is equal to the number of such $j$'s that $\lambda_j\neq\chi_0$ (with the notations in the proof of Theorem 2). Now let $D$ be an abelian subvariety of $A$, defined over $k$, such that any point $a$ on $A$ can be written as $a=d+c$ with $d$ in $D$ and $c$ in $C$ and $D\cap C$ is a finite subgroup of $A$. If $D_{\sigma_i}$ is the 0-component of the kernel of $\eta_{\sigma_i}-1$, then, as $\eta_{\sigma_i}-1$ has finite kernel on $C_{\sigma_i}$, $D_{\sigma_i}\cap C_{\sigma_i}$ is a finite subgroup of $A$ and so any point $a$ on $A$ can also be written as $a=d_i+c_i$ with $d_i$ in $D_{\sigma_i}$ and $c_i$ in $C_{\sigma_i}$. Hence $D$ is contained in $D_{\sigma_i}$ for any $\sigma_i$ in $G$. Taking a prime $l$ which does not divide the order of $D\cap C$, we have $\mathfrak{g}_l(A)=\mathfrak{g}_l(D)+\mathfrak{g}_l(C)$ (direct sum). Then as $D$ and $C$ are defined over $k$, and as $\eta_{\sigma_i}-1$ is 0 on $D$ and $(\eta_{\sigma_i}-1)C$ is contained in $C$ for any $\sigma_i$ in $G$, the matrices $M_l(\pi_A)$, $M_l(\eta_{\sigma_i}-1)$ and $M_l(\lambda)$ are of the following forms:

$$M_l(\pi_A)=\begin{pmatrix} M_l(\pi_D) & 0 \\ 0 & M_l(\pi_C)\end{pmatrix},\quad M_l(\eta_{\sigma_i}-1)=\begin{pmatrix} 0 & 0 \\ 0 & N_{\sigma_i}\end{pmatrix},$$
$$M_l(\lambda)=(\Lambda\quad 0),$$

where $\Lambda$ is a non-singular matrix of degree $2\cdot\dim D=2\cdot\dim B$; and clearly we have $\Lambda M_l(\pi_D)\Lambda^{-1}=M_l(\pi_B)$. Moreover, by the above argument, $2\cdot\dim D$ is equal to the number of such $j$'s that $\lambda_j=\chi_0$ and so all the characteristic roots of $N_{\sigma_i}$ are equal to $(\lambda_j(\sigma_i)-1)$'s with $\lambda_j\neq\chi_0$. As $B$ and the Albanese variety of $V$ have the same zeta-functions, we have the following additional statement to Theorem 2.

**Theorem 3.** *If $G$ is abelian and we write as usual* (*by Theorem 2*)

$$Z(u, V)=P_1(u)P_3(u)\cdots P_{2r-1}(u)/P_0(u)P_2(u)\cdots P_{2r}(u)\quad\textit{and}$$

$$Z(u, A(V)) = P_1'(u)P_3'(u)\cdots P_{2s-1}'(u)/P_0'(u)P_2'(u)\cdots P_{2s}'(u),$$

*where $A(V)$ is the Albanese variety of $V$ and $s$ is the dimension of $A(V)$, then we have the equality $P_1(u) = P_1'(u)$.*

**4.** Let $V$ be a normal algebraic variety of dimension $r$, defined over an algebraic number field $k$ of finite degree; let $A$ be an abelian variety such that $f: A \to V$ is a Galois covering, defined over $k$, with group $G$ and of degree $n$. We assume, moreover, that $V$ and $A$ are in some projective spaces. Then, by Shimura [4] and Taniyama [5], almost all primes $\mathfrak{p}$ in $k$ are 'non-exceptional' for the covering $A/V$ in the following sense: if we denote the reduction modulo $\mathfrak{p}$ of an object by the symbol $(\mathfrak{p})$, $f^{(\mathfrak{p})}: A^{(\mathfrak{p})} \to V^{(\mathfrak{p})}$ is a Galois covering, defined over $k^{(\mathfrak{p})}$, with the same group $G$ and of the same degree $n$ and $A^{(\mathfrak{p})}$ is an abelian variety defined over $k^{(\mathfrak{p})}$.

Then we can define the $L$-series $L(s, \chi, A/V)$ of the covering $A/V$ belonging to an irreducible character $\chi$ of $G$, by analogy with Hasse's zeta-functions of varieties, by

$$L(s, \chi, A/V) = \Pi_{\mathfrak{p}}' L((N\mathfrak{p})^{-s}, \chi, A^{(\mathfrak{p})}/V^{(\mathfrak{p})})$$

where $\mathfrak{p}$ ranges over all the non-exceptional primes for the covering $A/V$. Then the following theorem is an immediate consequence of Taniyama [5] and Theorem 2.

**Theorem 4.** *If $G$ is abelian and if $\mathcal{A}_0(A)$ contains a subfield of degree $2r$, then the zeta-function $\zeta_V(s)$ and the $L$-series $L(s, \chi, A/V)$ are expressed as products of $L$-functions of $k$ with 'Grössencharaktere' except for some factors of products of rational functions of $q^{-s}$ for a finite number of $q = N\mathfrak{p}$.*

## References


[1] E. Artin: Zur Theorie der $L$-Reihen mit allgemeinen Gruppencharakteren, Abh. Math. Sem. Univ. Hamburg, **8**, 292–306 (1930).

[2] S. Lang: Unramified class field theory over function fields in several variables, Ann. Math., **64**, 285–325 (1956).

[3] T. Matsusaka: On the algebraic construction of the Picard varieties II, Jap. Jour. Math., **22**, 51–62 (1952).

[4] G. Shimura: Reduction of algebraic varieties with respect to a discrete valuation of the basic field, Amer. Jour. Math., **77**, 134–176 (1955).

[5] Y. Taniyama: Jacobian varieties and number fields, Proc. Int. Symposium on Algebraic Number Theory, Tokyo-Nikko, 31–45 (1955).

[6] A. Weil: Variétés Abéliennes et Courbes Algébriques, Paris (1948).