Journal of the Mathematical Society of Japan Vol. 12, No. 1, January, 1960

On congruence L-series.

Dedicated to Professor Z. Suetuna on his 60th birthday.

By Makoto ISHIDA

(Received June 4, 1959)

Lang [3] has defined the congruence L-series $L(u, \chi, U/V)$ for a Galois covering $f: U\rightarrow V$ of an algebraic variety V defined over a finite field with q elements, associated with simple characters χ of the Galois group. Expressing their logarithmic derivatives as follows:

$$\frac{d}{du}\log L(u, \chi, U/V)=\sum_{\mu=1}^{\infty}c_{\mu}(\chi)u^{\mu-1},$$

Lang proved that the coefficients $c_{\mu}(\chi)$ satisfy some inequalities and explained the behavior of $L(u, \chi, U/V)$ in the disk $|u|<q^{-(r-1/2)}$, where r is the dimension of V (also of U). Moreover he gave a conjecture concerning the zeros of $L(u, \chi, U/V)$ on the circle $|u|=q^{-(r-1/2)}$. In the present paper, we shall prove that this conjecture holds under some assumption.

We shall first give another definition of $L(u, \chi, U/V)$. It can be shown that our definition is equivalent to Lang's, in the case where $f: U\rightarrow V$ is unramified and U is non-singular, after some cumbersome but not difficult calculations. Both definitions are not equivalent in general; but the L-series which we shall define will have the same behavior as Lang's L-series in the disk $|u|<q^{-(r-1)}$ in all cases, as will be shown by the birational nature of Corollary of Theorem 1 below. (We shall omit here the proof of equivalence of definitions for the unramified, non-singular case. Hereafter the notations $L(u, \chi, U/V)$ and $c_{\mu}(\chi)$ will be used to mean *our* L-series and their coefficients.)

Our definition of L-series will be given by the formulas (8) and (9) below, where $N_{\mu}(U, T_{\sigma})$ is the number of certain points on U, defined at the beginning of §1. Theorem 1 concerns a fundamental inequality on $N_{\mu}(U, T_{\sigma})$, which has important consequences on $c_{\mu}(\chi)$, as will be given as Corollary.

In view of the "birational equivalence" (in the sense above explained) of our definition with Lang's, the content of Corollary of Theorem 1 is covered by the result of [3]. So Theorem 1 could be also derived from the result of [3] simply by applying the orthogonality relations of group-characters. We prefer however to prove directly Theorem 1 by the same principle as in [3], since the method of this proof will be applied to a more general case in §2.

In § 2, we shall show that the analogue of the "trace formula" for $N_\mu(U, T_\sigma)$ and the conjecture of Lang explained above follow from the assumption (*). If the covering is trivial i. e. $U=V$, then our result is already obtained in Taniyama [**9**] under a weaker assumption than ours. (On an explicit form of the conjecture of Lang, see Ishida [**1**].)

In the following, we shall use the results of Lang [**3**] and Serre [**8**] often without references.

§ 1. A fundamental inequality.

1. Let U be a normal, projective variety of dimension r, defined over a finite field k with q elements; let T be a birational transformation of U into itself also defined over k. We suppose that T is everywhere defined on U and has a finite order n, i. e. T^n is the identity transformation of U. Let G be a cyclic group of biregular, birational transformations of U generated by T. Then, since U is projective and G is a finite group regularly operating on U, we can define the quotient variety $U_0=U/G$, which is also irreducible, normal, projective and of dimension r. Moreover we can construct U_0 and the canonical mapping f of U onto U_0 to be defined over the algebraic closure of k. Hence we may assume, by replacing k by a finite extension of k if necessary, that U_0 and f are also defined over k.

Let I_μ be the rational transformation of the ambient projective space of U given by the endomorphism of the universal domain: $\xi \rightarrow \xi^{q^\mu}$.

We denote by $N_\mu(U, T)$ the number of the points P on U such that $T(P) = I_\mu(P)$.

Theorem 1. *Let the notations be as explained above. Then there exist constants γ and δ such that, for any positive rational integer μ, we have the following inequality:*

(1) $$|N_\mu(U, T)-q^{\mu r}| \leqq \gamma q^{\mu(r-1/2)}+\delta q^{\mu(r-1)},$$

and the set of such constants γ is a birational invariant of U.

In § 2, we shall show that this constant γ is deeply related to the charactersitic roots of the l-adic representation of the automorphism of an Albanese variety of U given by T.

2. Now we prove Theorem 1. Let Z_0 be a k-closed algebraic subset of U_0 containing every point P_0 on U_0 which either ramifies in the Galois covering $f: U \rightarrow U_0$ or is multiple on U_0; then the dimension of Z_0 is less than r.

If P is a point on U such that $T(P)=I_\mu(P)$, then we have $f \cdot T(P)=f \cdot I_\mu(P)$; and so, as $f \cdot T=f$ and f is defined over k, we see that $P_0=f(P)$ is a rational point on U_0 over k_μ, the unique extension over k of degree μ.

Remark. Therefore, even in the case where U is not necessarily irreducible, we have

$$N_\mu(U, T) \leqq [U: U_0] \cdot N_\mu(U_0),$$

where $N_\mu(U_0)$ denotes the number of rational points on U_0 over k_μ. Hence *we have*, by Lang-Weil [**6**],

$$N_\mu(U, T) = O(q^{\mu r}).$$

In our proof, we shall first construct a suitable system of algebraic curves on U, each member of which is T-invariant.

Let $\boldsymbol{P}^*$ be the dual space of the ambient space $\boldsymbol{P}$ of U_0 and Γ the $(r-1)$-fold product of $\boldsymbol{P}^*$. Denoting the number of rational points on $\boldsymbol{P}$ over k by κ_{M+1}, we have

$$\kappa_{M+1} = \frac{q^{M+1}-1}{q-1},$$

where M is the dimension of $\boldsymbol{P}$. Clearly Γ has κ_{M+1}^{r-1} rational points over k. We need the following inequalities afterwards:

$$(2) \qquad \begin{aligned} &\left|\left(\frac{\kappa_{M+1}}{\kappa_M}\right)^{r-1} - q^{r-1}\right| \leqq c_1 q^{r-2}, \\ &q^{(M-1)(r-1)} \leqq \kappa_M^{r-1}, \end{aligned}$$

with a constant c_1, independent of q.

Any point v on Γ defines a linear variety L_v in $\boldsymbol{P}$. For a rational point P_0 on U_0 over k, there are exactly κ_M^{r-1} rational points a on Γ over k such that L_a contains P_0.

By Lang [**3**], there is a k-closed algebraic subset F of Γ such that, if a point v on Γ does not belong to F, the following three conditions are satisfied.

1) The intersection product $U_0 \cdot L_v = C_v$ is defined and is a non-singular irreducible curve on U_0.

2) The inverse image $f^{-1}(C_v) = W_v$ is an irreducible curve on U and simple on U. f_v (the restriction of f to W_v): $W_v \to C_v$ is a Galois covering with Galois group also generated by the restriction T_v of T to W_v and $[W_v: C_v] = [U: U_0]$. (Here W_v is not always normal, but we generalize the definition of Galois coverings.)

3) The intersection product $Z_0 \cdot C_v$ is defined and is an O-cycle on C_v. If a point P_0 on C_v does not belong to $Z_0 \cdot C_v$, then $f^{-1}(P_0)$ consists of $n = [W_v: C_v]$ different points on W_v, which are simple on W_v.

For a point v in F, we also denote $U_0 \cap L_v$ and $f^{-1}(U_0 \cap L_v)$ by C_v and W_v respectively. Those W_v's form a system of T-invariant curves on U, which we are looking for.

Denoting by $N(F)$ the number of rational points on F over k, we have, by Lang-Weil [**6**] and by the above inequality (2),

(3) $$N(F) \leqq c_2 q^{M(r-1)-1} \leqq c_2 \kappa_M^{r-1} q^{r-2},$$

with a constant c_2, independent of q.

As shown above, for any point P on U such that $T(P) = I_1(P)$, there are κ_M^{r-1} linear varieties L_a which contain $P_0 = f(P)$ and are defined over k. Hence there are κ_M^{r-1} curves C_a containing P_0 and defined over $\boldsymbol{k}$; and so there are also κ_M^{r-1} curves W_a containing the given P and defined over k.

Therefore we have

(4) $$N_1(U, T) = \frac{1}{\kappa_M^{r-1}} \sum_{a \in (\Gamma - F)_k} N_1(W_a, T_a) + \frac{1}{\kappa_M^{r-1}} \sum_{a \in F_k} N_1(W_a, T_a),$$

where the first and second sums range over all rational points on $\Gamma - F$ and F over k respectively.

3. Let a belong to F and be rational over k. Then we have, by the remark given above,

$$N_1(W_a, T_a) \leqq n \cdot N_1(C_a),$$

where $N_1(C_a)$ denotes the number of rational points on C_a over k. On the other hand, by Lang [**3**], we have

$$\left| \frac{1}{\kappa_M^{r-1}} \sum_{a \in F_k} N_1(C_a) \right| \leqq c_3 q^{r-1/2},$$

with a constant c_3, independent of q. Therefore we have

(5) $$\left| \frac{1}{\kappa_M^{r-1}} \sum_{a \in F_k} N_1(W_a, T_a) \right| \leqq n \cdot c_3 q^{r-1/2}.$$

Let a belong to $\Gamma - F$ and be rational over k. Let $W_a{}^*$ be a non-singular irreducible curve, birationally equivalent to W_a over k. Then the number of points, at which the birational transformation between W_a and $W_a{}^*$ is not biregular, is less than $[W_a : C_a] \deg(C_a \cdot Z_0)$, by the condition 3); hence it is uniformly bounded. The genus $g_a{}^*$ of $W_a{}^*$ is also uniformly bounded. Moreover T_a induces naturally a biregular, birational transformation $T_a{}^*$ of $W_a{}^*$, which has also a finite order. Clearly we have

$$| N_1(W_a, T_a) - N_1(W_a{}^*, T_a{}^*) | \leqq c_4,$$

with a constant c_4, independent of a. On the other hand, since the degree of the automorphism $T_a{}^*$ is 1, we have, by Weil (or more explicitly by Mattuck-Tate [**7**]),

$$| N_1(W_a{}^*, T_a{}^*) - q | \leqq 2 g_a{}^* q^{1/2} + 1 \leqq c_5 q^{1/2},$$

with a constant c_5, independent of q and a. Hence we have

(6) $$| N_1(W_a, T_a) - q | \leqq c_6 q^{1/2},$$

with a constant c_6, independent of q and a. On the other hand, we have, by (2) and (3),

$$\left|\frac{1}{\kappa_M^{r-1}}\sum_{a\in(\Gamma-F)_k}1-q^{r-1}\right|=\left|\frac{\kappa_{M+1}^{r-1}-N(F)}{\kappa_M^{r-1}}-q^{r-1}\right|\leqq c_7q^{r-2}, \tag{7}$$

with a constant c_7, independent of q.

Therefore we have, by (4), (5), (6) and (7),

$$|N_1(U,T)-q^r|\leqq\gamma q^{r-1/2}+\delta q^{r-1},$$

with constants γ and δ, independent of q.

If we extend the ground field k to its finite extension k_μ with q^μ elements, we have also an estimation of $N_\mu(U,T)$ as stated in Theorem 1.

Moreover if X is a T-invariant k-closed algebraic subset of U, then it is clear that we have, by the remark in **2**,

$$|N_\mu(U,T)-N_\mu(U-X,T)|\leqq c_8q^{\mu(r-1)},$$

with a constant c_8, independent of μ. Therefore the set of such constants γ is a birational invariant of U.

Thus the proof of Theorem 1 is completed.

4. Let $f: U\rightarrow V$ be a Galois covering of degree n, defined over a finite field k with q elements, where U and V are normal, projective varieties of dimension r. The elements of the Galois group G will be denoted by T_σ, $T_\tau,\cdots$. Then, by the definition of Galois coverings, the numbers $N_\mu(U,T_\sigma)$, $N_\mu(U,T_\tau),\cdots$ are well defined.

For a simple character χ of G, we define the congruence L-series $L(u,\chi,U/V)$ by the following logarithmic derivative:

$$\frac{d}{du}\log L(u,\chi,U/V)=\sum_{\mu=1}^{\infty}c_\mu(\chi)u^{\mu-1}, \tag{8}$$

and by the condition $L(O,\chi,U/V)=1$, where the coefficients $c_\mu(\chi)$ are given by

$$c_\mu(\chi)=\frac{1}{n}\sum_{T_\sigma\in G}\chi(T_\sigma)N_\mu(U,T_\sigma). \tag{9}$$

Then, by the orthogonality relations of group-characters and Theorem 1, we have the following

COROLLARY. *We have, for every positive rational integer* μ,

$$\begin{aligned}&|c_\mu(\chi)|\leqq\gamma_\chi q^{\mu(r-1/2)}+\delta_\chi q^{\mu(r-1)},\ \textit{if } \chi \textit{ is not principal,}\\ &|c_\mu(\chi_0)-q^{\mu r}|\leqq\gamma_{\chi_0}q^{\mu(r-1/2)}+\delta_{\chi_0}q^{\mu(r-1)},\ \textit{if } \chi_0 \textit{ is principal,}\end{aligned} \tag{10}$$

where γ_χ *and* δ_χ *are constants, independent of* μ. *Therefore* $L(u,\chi,U/V)$ *with* $\chi\neq\chi_0$ *have neither zero nor pole in the disk* $|u|<q^{-(r-1/2)}$.

§ 2. The conjecture of Lang.

5. Let the notations be as explained in **1**. By Theorem 1, we can write

$$N_\mu(U, T)=q^{\mu r}+\gamma_\mu q^{\mu(r-1/2)}+O(q^{\mu(r-1)}), \tag{11}$$

for each μ, where γ_μ are constants bounded in absolute value by a fixed constant γ.

Let $U(m)$ be the m-fold symmetric product of U; we may assume that $U(m)$ is also defined over k. Then T induces naturally a biregular, birational transformation of $U(m)$ into itself, which has the same order n. Let h be the canonical mapping of the m-fold product $U\times U\times\cdots\times U$ of U onto $U(m)$ and let Δ be the diagonal of $U\times U$. Then $X=h(\Delta\times U\times\cdots\times U)$ is a subvariety of $U(m)$ and has the dimension $(m-1)r$. Clearly X is invariant by T and I_μ for all μ. Any point $\mathfrak{a}$ on $U(m)-X$ has a representative $(P_1, P_2, \cdots, P_m)$ with points P_i on U, where any two of the points $P_1, \cdots, P_m$ are different from each other.

Let $\mathfrak{a}$ be a point on $U(m)-X$ such that $T(\mathfrak{a})=I_\mu(\mathfrak{a})$, where I_μ denotes also the q^μ-th power transformation of the ambient space of $U(m)$. If $(P_1, \cdots, P_m)$ is a representative of $\mathfrak{a}$, then, by a suitable change of indices, the points $P_1, \cdots, P_m$ are divided into several sets as follows:

$$T(P_1)=I_\mu(P_2),\ T(P_2)=I_\mu(P_3), \cdots, T(P_{\rho_1})=I_\mu(P_1);$$
$$T(P_{\rho_1+1})=I_\mu(P_{\rho_1+2}), \cdots, T(P_{\rho_1+\rho_2})=I_\mu(P_{\rho_1+1});$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

where $\sum\rho_i$ equals to m and ρ_i is a positive rational integer. Then $\mathfrak{a}$ is called to be "of type $(\rho_1, \rho_2, \cdots)$" and $(P_1, \cdots, P_{\rho_1}), (P_{\rho_1+1}, \cdots, P_{\rho_1+\rho_2}), \cdots$ are called "cycles of length $\rho_1, \rho_2, \cdots$ of $\mathfrak{a}$" respectively. We denote by $[\mathfrak{a}]$ the number of cycles of $\mathfrak{a}$.

Let $(P_1, \cdots, P_\rho)$ be a cycle of length ρ of some point $\mathfrak{a}$ on $U(m)-X$ such that $T(\mathfrak{a})=I_\mu(\mathfrak{a})$. As T is defined over k, we have $T\cdot I_\mu=I_\mu\cdot T$ and so

$$T^\rho(P_1)=I_{\rho\mu}(P_1) \tag{12}$$

and $P_\rho=T^{-1}I_\mu(P_1), \cdots, P_2=(T^{-1}I_\mu)^{\rho-1}(P_1)$ are uniquely determined by P_1. Moreover, as $\mathfrak{a}$ is in $U(m)-X$, any two of $P_1, \cdots, P_\rho$ are different from each other. Hence ρ is the smallest value with which P_1 satisfies (12).

It is easily verified, by Theorem 1, that the number of points on U, which satisfy (12) with ρ as the smallest value, is given by

$$N_{\rho\mu}(U, T^\rho)+O(q^{\mu(\rho-1)r}). \tag{13}$$

Conversely if a point P on U satisfies (12) with ρ as the smallest value, then any two of $(T^{-1}I_\mu)^\nu(P)$ with $\nu=0, 1, \cdots, \rho-1$ are different from each other.

Hence, by (13), $(P, (T^{-1}I_\mu)^{\rho-1}(P), \cdots, (T^{-1}I_\mu)(P))$ appears as a cycle of length ρ of some point $\mathfrak{a}$ on $U(m)-X$ such that $T(\mathfrak{a})=I_\mu(\mathfrak{a})$ and $[\mathfrak{a}]=s$, where s is any positive rational integer not larger than $m-\rho+1$.

Hence the number of points $\mathfrak{a}$ on $U(m)-X$, such that $T(\mathfrak{a})=I_\mu(\mathfrak{a})$ and $[\mathfrak{a}]=s$, is given by

$$\frac{1}{s!}\sum_{\substack{(\rho_1,\cdots,\rho_s)\\ \rho_1+\cdots+\rho_s=m}} \frac{N_{\rho_1\mu}(U, T^{\rho_1})}{\rho_1}\cdots\frac{N_{\rho_s\mu}(U, T^{\rho_s})}{\rho_s}+O(q^{\mu(m-1)r}). \tag{14}$$

Here the sum $\sum\limits_{\substack{(\rho_1,\cdots,\rho_s)\\ \rho_1+\cdots+\rho_s=m}}$ ranges over all the s-permutations $(\rho_1, \cdots, \rho_s)$ of positive rational integers with $\sum\limits_{i=1}^{s}\rho_i=m$, where each of the s integers may be repeated. Moreover the error term of (14) is due to that of (13) and the fact that our consideration is restricted to points on $U(m)-X$.

Therefore, by the above arguments and the remark in **2**, we have the following formula (cf. Taniyama [**9**]):

$$\begin{aligned} N_\mu(U(m), T) &= N_\mu(U(m)-X, T)+O(q^{\mu(m-1)r}) \\ &= \frac{N_{m\mu}(U, T^m)}{m}+\frac{1}{2!}\sum_{\substack{(\rho_1,\rho_2)\\ \rho_1+\rho_2=m}}\frac{N_{\rho_1\mu}(U, T^{\rho_1})}{\rho_1}\cdot\frac{N_{\rho_2\mu}(U, T^{\rho_2})}{\rho_2} \\ &\quad+\frac{1}{3!}\sum_{\substack{(\rho_1,\rho_2,\rho_3)\\ \rho_1+\rho_2+\rho_3=m}}\frac{N_{\rho_1\mu}(U, T^{\rho_1})}{\rho_1}\cdot\frac{N_{\rho_2\mu}(U, T^{\rho_2})}{\rho_2}\cdot\frac{N_{\rho_3\mu}(U, T^{\rho_3})}{\rho_3} \\ &\quad+\cdots+\frac{N_\mu(U, T)^m}{m!}+O(q^{\mu(m-1)r}). \end{aligned} \tag{15}$$

We note that, as r is larger than 0, we have $(m-1)r\leqq mr-1$.

On the other hand, by Theorem 1, we have

$$|N_\mu(U(m), T)-q^{\mu mr}|\leqq\gamma^* q^{\mu(mr-1/2)},$$

with a constant γ^*, independent of μ. Hence, comparing the coefficients of $q^{\mu mr}$ in the both sides of the above expression (15) of $N_\mu(U(m), T)$, we have

$$1=\frac{1}{m}+\frac{1}{2!}\sum_{\substack{(\rho_1,\rho_2)\\ \rho_1+\rho_2=m}}\frac{1}{\rho_1}\frac{1}{\rho_2}+\frac{1}{3!}\sum_{\substack{(\rho_1,\rho_2,\rho_3)\\ \rho_1+\rho_2+\rho_3=m}}\frac{1}{\rho_1}\frac{1}{\rho_2}\frac{1}{\rho_3}+\cdots+\frac{1}{m!}. \tag{16}$$

As $\mu\Big((m-\rho_i)r+\rho_i r-\dfrac{1}{2}\rho_i\Big)=\mu\Big(mr-\dfrac{1}{2}\rho_i\Big)$, a term of order $q^{\mu(mr-1/2)}$ appears in $N_{\rho_1\mu}(U, T^{\rho_1})\cdot N_{\rho_2\mu}(U, T^{\rho_2})\cdots N_{\rho_s\mu}(U, T^{\rho_s})$ with $\sum\limits_{i=1}^{s}\rho_i=m$ if and only if some ρ_i is equal to 1. Hence, if m is larger than 1, the sum of the terms of order $q^{\mu(mr-1/2)}$ in the right side of (15) is given by

$$\frac{2}{2!}\frac{1}{m-1}\gamma_\mu q^{\mu(r-1/2)+\mu(m-1)r}+\frac{3}{3!}\sum_{\substack{(\rho_1,\rho_2)\\ \rho_1+\rho_2=m-1}}\frac{1}{\rho_1}\frac{1}{\rho_2}\gamma_\mu q^{\mu(r-1/2)+\mu(m-1)r}$$
$$+\cdots+\frac{m}{m!}\gamma_\mu q^{\mu(r-1/2)+\mu(m-1)r}$$
$$=\left\{\frac{1}{m-1}+\frac{1}{2!}\sum_{\substack{(\rho_1,\rho_2)\\ \rho_1+\rho_2=m-1}}\frac{1}{\rho_1}\frac{1}{\rho_2}+\cdots+\frac{1}{(m-1)!}\right\}\gamma_\mu q^{\mu(mr-1/2)}$$
$$=\gamma_\mu q^{\mu(mr-1/2)}$$

by the formula (16) for $m-1$.

Therefore we have also

$$N_\mu(U(m),T)=q^{\mu mr}+\gamma_\mu q^{\mu(mr-1/2)}+O(q^{\mu(mr-1)}).$$

6. Now we shall restrict ourselves to the case where U is non-singular and T satisfies the following condition: If the a-th power T^a of T leaves at least one point on U fixed, then a is divisible by the order n of T. This condition imposed on T is always satisfied when T is an element of the Galois group of some unramified Galois covering. However, in order to study the constant γ in Theorem 1, these assumptions are not essential, because of the birationality of the constants γ.

We choose m to be prime to n. We suppose that, for a positive rational integer a not divisible by n, there exists a point $\mathfrak{a}$ on $U(m)$ which is fixed by T^a. Let $(P_1,P_2,\cdots,P_m)$ be a representative of $\mathfrak{a}$; then we may assume that the points $P_1,\cdots,P_m$ are divided into several sets as follows:

$$T^a(P_1)=P_2,\quad T^a(P_2)=P_3,\quad\cdots,\quad T^a(P_{\rho_1})=P_1;$$
$$T^a(P_{\rho_1+1})=P_{\rho_1+2},\quad\cdots,\quad T^a(P_{\rho_1+\rho_2})=P_{\rho_1+1};$$
$$\cdots\cdots\cdots\cdots\cdots\cdots,$$

where $\sum\rho_i$ equals to m and ρ_i is a positive rational integer. Then we have

$$T^{a\rho_1}(P_1)=P_1,\quad T^{a\rho_2}(P_{\rho_1+1})=P_{\rho_1+1},\cdots.$$

Hence, by the assumption of T, each $a\rho_i$ must be divisible by n; so $am=\sum a\rho_i$ is divisible by n, which contradicts to our choice of m. Therefore we can choose m so that if a is not divisible by n then T^a has no fixed point on $U(m)$.

Let A be an Albanese variety attached to U and α a canonical mapping of U into A. As k is finite, A and α may be assumed to be defined over k. A is also an Albanese variety attached to $U(m)$ and α induces naturally a canonical mapping α_m of $U(m)$ into A. For a generic point P on U over k, we have, by the universal mapping property of Albanese varieties,

$$\alpha\cdot T(P)=\eta\cdot\alpha(P)+t,$$

where η is an automorphism of A defined over k and t is a rational point on A over k, which are independent of the choice of P. So, for a generic point $\mathfrak{u}$ on $U(m)$ over k, we have

$$\alpha_m \cdot T(\mathfrak{u}) = \eta \cdot \alpha_m(\mathfrak{u}) + mt .$$

We note that α and α_m are everywhere defined on U and $U(m)$ respectively because U is non-singular by our assumption.

If a point $\mathfrak{a}$ on $U(m)$ satisfies $T(\mathfrak{a}) = I_\mu(\mathfrak{a})$, then we have $\alpha_m \cdot T(\mathfrak{a}) = \alpha_m \cdot I_\mu(\mathfrak{a})$. As α_m is defined over k, we have

$$\eta \cdot \alpha_m(\mathfrak{a}) + mt = \pi^\mu \alpha_m(\mathfrak{a}) ,$$

where π is the endomorphism of A given by the endomorphism of the universal domain: $\xi \rightarrow \xi^q$.

Now we choose m to be prime to n and sufficiently larger than $2g+2$, where g is the dimension of A. For a point a on A, $W(m, a)$ denotes the subvariety of $U(m)$ consisting of all points $\mathfrak{a}$ such that $\alpha_m(\mathfrak{a}) = a$. Then, for our choice of m, $W(m, a)$ is irreducible and of dimension $mr-g$, by Taniyama [**9**].

We denote also by $N_\mu(W(m, a), T)$ the number of points $\mathfrak{a}$ on $W(m, a)$ such that $T(\mathfrak{a}) = I_\mu(\mathfrak{a})$. Since T does not generally map $W(m, a)$ into itself and also $W(m, a)$ is not generally defined over k, we can not apply Theorem 1 to this case. However, for such a point a on A that $\eta(a) + mt = \pi^\mu(a)$, we have an analogous inequality as we shall show afterwards.

By the above arguments and the fact that T and α_m are everywhere defined on $U(m)$, we have

$$N_\mu(U(m), T) = \sum_a N_\mu(W(m, a), T) , \tag{17}$$

where the sum ranges over all points a on A such that

$$\eta(a) + mt = \pi^\mu(a) .$$

We note that there are exactly $\det M_l(\pi^\mu - \eta)$ such points a on A, where M_l denotes the l-adic representation of the ring of endomorphisms of A with a rational prime l different from the characteristic of the universal domain. In fact, if x is a generic point on A over k, we have $k(\eta(x)) = k(x)$ and so $k(\pi^\mu(x), (\pi^\mu - \eta)(x)) = k(x)$; hence we have $\nu_i(\pi^\mu - \eta) = 1$ and so $\nu_s(\pi^\mu - \eta) = \det M_l(\pi^\mu - \eta)$.

7. Now we shall calculate the number $N_\mu(W(m, a), T)$ for a point a on A such that $\eta(a) + mt = \pi^\mu(a)$.

Since $U(m)$ is projective and the cyclic group generated by T is a finite group of biregular, birational transformations of $U(m)$ into itself, we can define the quotient variety; and then, by our choice of m, we have an unramified Galois covering and we may assume that this covering is defined over k. W_0 denotes the image of $W(m, a)$ by the canonical projection f of this covering.

By the definition, $T(W(m, a))$ coincides with $W(m, \eta(a)+mt) = W(m, \pi^{\mu}(a))$; and, as α_m is defined over k, $I_{\mu}(W(m, a))$ coincides with $W(m, \pi^{\mu}(a))$ and consequently with $T(W(m, a))$. It is clear, by considering the dimensions, $W(m, a)$ and $T(W(m, a)) = I_{\mu}(W(m, a))$ are irreducible components of the inverse image $f^{-1}(W_0)$. Hence, as f is defined over k and $f \cdot T = f$, it is easily verified that W_0 is defined over k_{μ}. Moreover, let $W_1 = W(m, a)$, $W_2 = T(W(m, a))$, $W_3, \cdots$ be all the irreducible components of the inverse image $f^{-1}(W_0)$. Since each W_i is written as $W(m, b_i)$ with some point b_i on A and so the intersection $W_i \cap W_j$ is empty for distinct b_i and b_j, any two of W_i's have no point in common. Then, by Lang-Serre [4] and [5], we have $\sum_i [W_i : W_0]_s \leqq n$, where n is the degree of the covering and the symbol $[W_i : W_0]_s$ denotes the separable part of the degree $[W_i : W_0]$. We note that $[W_i : W_0]_s$ is equal to the number of points on W_i lying over a generic point of W_0. As $W_i \cap W_j$ is empty and the covering is unramified, we have $n = \sum_i [W_i : W_0]_s$ and so, by the remark in [5], we have $[W_i : W_0]_s = [W_i : W_0]$. Especially it follows that the function fields of $W(m, a)$ and of $T(W(m, a))$ are separable over that of W_0. Hence we can conclude that $f_1 : W(m, a) \rightarrow W_0$ and $f_2 : T(W(m, a)) \rightarrow W_0$ are unramified coverings, where f_1 and f_2 are the restrictions of f on $W(m, a)$ and $T(W(m, a))$ respectively. (If necessary, we may replace $W(m, a)$, $T(W(m, a))$ and W_0 by their normalizations, because of the birational nature of the following statements.) Let C_u' be a generic hyperplane section curve on W_0 over k_{μ} with defining coefficients (u) and W_u' the inverse image $f_1^{-1}(C_u')$ contained in $W(m, a)$. Then $T(W_u')$ coincides with the inverse image $f_2^{-1}(C_u')$ contained in $T(W(m, a))$. Let C_b' be a specialization of C_u' over a specialization $(u) \rightarrow (b)$ with reference to k_{μ} and be rational over k_{μ}. For almost all such C_b', by similar arguments as in **2**, $W_b' = f_1^{-1}(C_b')$ and $T(W_b') = f_2^{-1}(C_b')$ are irreducible curves on $W(m, a)$ and $T(W(m, a))$ respectively. As f and C_b' are defined over k_{μ}, $I_{\mu}(W_b')$ is contained in $I_{\mu}(W(m, a)) = T(W(m, a))$ and has the projection C_b' on W_0; so $I_{\mu}(W_b')$ must coincide with $T(W_b')$. Also, by Weil or by Mattuck-Tate [7], we have, for almost all such W_b',

$$|N_{\mu}(W_b', T) - q^{\mu}| \leqq c_9 q^{\mu/2} + 1 ,$$

with a constant c_9, independent of q and (b). Therefore, by the same principle as in the proof of Theorem 1, we have

$$(18) \qquad |N_{\mu}(W(m, a), T) - q^{\mu s}| \leqq \gamma_a' q^{\mu(s-1/2)} + \delta_a' q^{\mu(s-1)} ,$$

with constants γ_a' and δ_a', independent of q, where $s = mr - g$ is the dimension of $W(m, a)$.

It is known that $W(m, a)$ is a regular variety, i.e. an Albanese variety attached to $W(m, a)$ is trivial (cf. Koizumi [**2**]). So, as a special case of analogues of the conjecture of Lang, we assume that the following conjecture holds.

We have, for every a on A such that $\eta(a)+mt=\pi^{\mu}(a)$,

$$(*) \qquad |N_{\mu}(W(m, a), T)-q^{\mu s}| \leqq \gamma_0 q^{\mu(s-1)},$$

where γ_0 is a constant, inedependent of μ and a.

Let $\pi_1, \pi_2, \cdots, \pi_{2g}$ and $\zeta_1, \zeta_2, \cdots, \zeta_{2g}$ be the characteristic roots of $M_l(\pi)$ and $M_l(\eta)$ respectively, where $|\pi_i|=q^{1/2}$ and ζ_i is a n-th root of unity. Then, as $\eta\pi^{\mu}=\pi^{\mu}\eta$ for all μ, it is easily verified that, by a suitable change of indices, $\pi_1{}^{\mu}-\zeta_1, \pi_2{}^{\mu}-\zeta_2, \cdots, \pi_{2g}{}^{\mu}-\zeta_{2g}$ are the characteristic roots of $M_l(\pi^{\mu}-\eta)$. Then, by (17) in the end of **6** and by the fact that $\pi_1\pi_2\cdots\pi_{2g}=\det M_l(\pi)=q^g$, we have, under the assumption (*),

$$N_{\mu}(U(m), T)=q^{\mu mr}-\sum_{i=1}^{2g}(q^{mr}\pi_i{}^{-1})^{\mu}\zeta_i+O(q^{\mu(mr-1)}).$$

Therefore, using the notations and results in **5**, we have, for each μ,

$$\gamma_{\mu}q^{\mu(mr-1/2)}=-\sum_{i=1}^{2g}(q^{mr}\pi_i{}^{-1})^{\mu}\zeta_i+O(q^{\mu(mr-1)}),$$

and so

$$\gamma_{\mu}q^{\mu(r-1/2)}=-\sum_{i=1}^{2g}(q^{r}\pi_i{}^{-1})^{\mu}\zeta_i+O(q^{\mu(r-1)}).$$

Hence we have the following

THEOREM 2. *The notations be as explained above. Then we have, under the assumption (*),*

$$(19) \qquad N_{\mu}(U, T)=q^{\mu r}-\sum_{i=1}^{2g}(q^{r}\pi_i{}^{-1})^{\mu}\zeta_i+O(q^{\mu(r-1)}).$$

Repeating the same calculations of $\det M_l(\pi^{\mu}-\eta)$ as in Ishida [**1**], we have also the following

COROLLARY. *Let $f: U\to V$ be an unramified Galois covering defined over a finite field k with q elements, where U and also V are non-sigular, projective varieties of dimension r. Then, concerning the zeros of $L(u, \chi, U/V)$ on the circle $|u|=q^{-(r-1/2)}$, the conjecture of Lang holds under the assumption (*) on U.*

Department of Mathematics
University of Tokyo.

References

[1] M. Ishida, On zeta-functions and L-series of algebraic varieties II, Proc. Japan Acad., **34** (1958), 395-399.

[2] S. Koizumi, On Albanese varieties, to appear in Illinois J. Math.

[3] S. Lang, Sur les séries L d'une variété algébrique, Bull. Soc. Math. France, **84** (1956), 385-407.

[4] S. Lang-J. P. Serre, Sur les revêtements non ramifiés des variétés algébriques, Amer. J. Math., **79** (1957), 319-330.

[5] S. Lang-J. P. Serre, Errata, Amer. J. Math., **81** (1959), 279-280.

[6] S. Lang-A. Weil, Number of points of varieties in finite fields, Amer. J. Math., **76** (1954), 819-827.

[7] A. Mattuck-J. Tate, On the inequality of Castelnuovo-Severi, Abh. Math. Semi. Univ. Hamburg, **22** (1958), 295-299.

[8] J. P. Serre, Groupes algébriques et théorie du corps de classes, Lecture note at Collège de France, 1957.

[9] Y. Taniyama, Distribution of positive 0-cycles in absolute classes of an algebraic variety with finite constant fields, Sci. Papers Coll. Gen. Ed., Univ. Tokyo, **8** (1958), 123-137.