II

AMERICAN MATHEMATICAL SOCIETY

Lecture Notes Prepared in Connection With the

Summer Institute on

Algebraic Geometry

held at the

Whitney Estate, Woods Hole, Massachusetts

July 6 - July 31, 1964

TABLE OF CONTENTS

# ÉTALE COHOMOLOGY OF SCHEMES

by M. Artin

A topology $T$ consists of a category $C$ and a collection of families of maps of $C$. The objects of the category are to be thought of as "open sets", and the distinguished families of maps as "coverings" of one open set by another. There are a few mild axioms to be put on the situation, such as that a restriction of a covering is again a covering (see [ 1 ] for precise definitions). A sheaf $F$ on a topology is a contravariant functor on $C$, e.g., to abelian groups, having the sheaf property that whenever a family $\{ X_i \xrightarrow{f_i} X \}$ of maps of $C$ is a covering the sequence of abelian groups

$$0 \longrightarrow F(X) \xrightarrow{\prod F(f_i)} \prod_i F(X_i) \xrightarrow{\prod (F(pr_1) - F(pr_2))} \prod_{i,j} F(X_i \times_X X_j)$$

is exact. Most of sheaf theory goes through in this setting, and in particular one has cohomology theory.

For the étale topology on a prescheme $X$ one takes as "open sets" the étale morphisms $X' \longrightarrow X$. A family of maps $\{ X'_i \to X' \}$ over $X$ is called a covering if $X' = \bigcup_{\text{set}} \text{im}(X'_i)$ theoretically the union of the images of the $X_i$'s.

Let us suppose that $f : X' \longrightarrow X$ is a morphism of preschemes of finite type over Spec $\mathbb{C}$, $\mathbb{C}$ the field of complex numbers. Then $f$ is étale if and only if the associated map of the underlying complex analytic spaces is a local isomorphism, i.e., if and only if every point $x'$ of $X'$ has an open neighborhood which is mapped isomorphically onto an open subspace of $X$. Now as far as the category of sheaves is concerned, there is no difference between the usual topology on a topological space and the one obtained by taking as open sets the local isomorphisms. This is because obviously every covering in the

latter sense is dominated by one in the former sense. Therefore the étale topology on an algebraic prescheme $X$ over Spec $\mathbb{C}$ is a straightforward algebraic version of the classical topology for analytic spaces. One has a "continuous map"

$$\varepsilon : X_{class} \to X_{étale},$$

and the following result holds.

Theorem: Let $X$ be of finite type over Spec $\mathbb{C}$ and let $F$ be a noetherian torsion sheaf on $X_{étale}$. Then the cohomology maps

$$H^q(X_{étale}, F) \to H^q(X_{class}, \varepsilon^* F)$$

induced by $\varepsilon$ are isomorphisms for each $q$.

This theorem in its general form requires resolution of singularities. The étale cohomology theory does not give the classical answers for a non-torsion sheaf such as the constant sheaf $\mathbb{Z}$.

In general, most results of a basic sort are known by now, except that certain facts require resolution of singularities, and the cohomology behaves perfectly for torsion sheaves prime to the residue characteristics. One has for example the specialization theorem.

Theorem: Let $X$ be a prescheme smooth and proper over a base $S$. Then the cohomologies of the geometric fibres $H^q(X_{\bar{s}}, \mathbb{Z}/n)$ are isomorphic for $n$ prime to the residue characteristics.

Elementary Theory:

Case $X$ = Spec k, k a field: Here the situation is very nice. An étale map $X' \to X$ is just the spectrum of a finite separable k-algebra $k'$, so although the topology is far from trivial, it is fairly explicitly known. The main

result is that the category of sheaves on $X$ for the étale topology is equivalent with the category of continuous $G$-modules where $G = G(\bar{k}/k)$ is the galois group of the separable algebraic closure $\bar{k}$ of $k$. Hence the cohomology is the ordinary galois cohomology developed by Tate [5].

Kummer Theory: There is a sheaf $(\mathbb{G}_m)_X$ whose sections on an $X'$ étale over $X$ are the units in the structure sheaf $\Gamma(X', \mathcal{O}_{X'})$ (one has to check that this is a sheaf). One has

Hilbert Theorem 90: $H^1(X, (\mathbb{G}_m)_X) = \operatorname{Pic} X$ is the group of isomorphism classes of invertible sheaves on $X$. Hence the cohomology in low dimensions of $(\mathbb{G}_m)_X$ is known. This gives information about cohomology with values in constant sheaves because of Kummer Theory: One has the $n$th power map $(\mathbb{G}_m)_X \xrightarrow{n} (\mathbb{G}_m)_X$. Suppose that $n$ is prime to the residue characteristics of $X$. Then this map is surjective as a map of sheaves. In fact, if $u$ is a unit on an $X'$ then the algebra

$$\mathcal{O}_{X'}[t]/(t^n - u)$$

defines an étale surjective extension of $X'$, hence $u$ is "locally for the étale topology" an $n$th power. One has therefore an exact sequence.

Kummer Theory: $\quad 0 \to (\mu_n)_X \to (\mathbb{G}_m)_X \xrightarrow{n} (\mathbb{G}_m)_X \to 0$

where $(\mu_n)_X$ is the sheaf of $n$th roots of unity. The sheaf $(\mu_n)_X$ is locally (non-canonically) isomorphic to the constant sheaf $\mathbb{Z}/n$.

Case $X$ is an algebraic curve: Let $k$ be a separably algebraically closed field and $X$ an algebraic curve over $\operatorname{Spec} k$, say reduced and irreducible.

Theorem: $\quad H^q(X, (\mathbb{G}_m)_X) \underset{p}{=} 0, \quad q > 1$

where $\underset{p}{=} 0$ means that the group is a $p$-torsion group, $p = \operatorname{char} k$.

Corollary: Applying Kummer theory, the cohomology of $X$ with values in $(\mu_n)_X$, $(n,p) = 1$, is given by the exact sequence

$$0 \to \mu_n \to \Gamma(X, \mathcal{O}_X)^* \xrightarrow{n} \Gamma(X, \mathcal{O}_X)^* \to H^1(X, \mu_n) \to \operatorname{Pic} X \downarrow n$$
$$0 \leftarrow H^2(X, \mu_n) \leftarrow \operatorname{Pic} X$$

In particular, if $X$ is complete and nonsingular then $\Gamma(X, \mathcal{O}_X)^* = k^*$ is divisible by $n$ and one finds

$H^0(X, \mu_n) = (\mu_n)_k$ = a cyclic group of order $n$.

$H^1(X, \mu_n) = A_n$ = group of points of order $n$ on the jacobian $A$ of $X$

$H^2(X, \mu_n) = \mathbb{Z}/n = \operatorname{Pic} X / n \operatorname{Pic} X$.

Proof of the theorem: Let $i: P \to X$ be the inclusion of the general point of $X$. There is an obvious inclusion $(\mathbb{G}_m)_X \to i_*(\mathbb{G}_m)_P$, and hence an exact sequence

$$0 \to (\mathbb{G}_m)_X \to i_*(\mathbb{G}_m)_P \to D \to 0$$

where $D$ is the cokernel. The sheaf $D$ has the property that every section is zero outside a finite number of points, i.e., $D$ is a "skyscraper" sheaf. One can show that therefore $H^q(X, D) = 0$, $q > 0$. Hence, it suffices to show

$$H^q(X, i_*(\mathbb{G}_m)_P) = 0, \quad q > 0$$

which can be handled because $P = \operatorname{Spec} K$ is the spectrum of the function field of $X$. Consider the Leray spectral sequence

$$H^p(X, R^q i_*(\mathbb{G}_m)_P) \Rightarrow H^{p+q}(P, (\mathbb{G}_m)_P).$$

Because of Hilbert Theorem 90 and dimension theory for galois cohomology (Tsen's theorem in particular), $H^r(P, (\mathbb{G}_m)_P) \underset{p}{=} 0$, $r > 0$. Thus it suffices to show that also $R^q i_*(\mathbb{G}_m)_P \underset{p}{=} 0$, $q > 0$. But $R^q i_*(\mathbb{G}_m)_P$ is the sheaf associated to the presheaf which attaches to an $X'/X$ the group

$H^q(X^1 \times_X P, (\mathbb{G}_m)_P)$. Here $X^1 \times_X P$ is the spectrum of a separable extension of $K$, i.e., a direct product of function fields of algebraic curves, i.e., is similar to $P$. Hence $H^q(X^1 \times_X P, (\mathbb{G}_m)_P) \underset{p}{=} 0$, $q > 0$, and so $R^q i_*(\mathbb{G}_m)_P \underset{p}{=} 0$, $q > 0$ as required.

By general nonsense methods, one can reduce most questions in the study of torsion sheaves to the case of a constant sheaf such as $\mu_n$, and so Kummer theory gives a good hold on dimension 1. The results in this case are more or less old stuff, similar situations having been studied by Tate [5], Ogg [3] and Šafarevič [4].

Higher dimension and the proper base change theorem.

The case of varieties of dimension $> 1$ is much more difficult than that of dimension 1. In fact, it is far from trivial to calculate the cohomology of the projective or affine space of dimension 2. One obvious approach to the problem of calculating the cohomology of a variety $X$ of dimension $n > 1$ is to map $X$ to $\mathbb{P}^1$ by a nonconstant function and to proceed by induction on $n$ -- the fibres of the map will be of dimension $(n-1)$. This leads to the general problem of calculating the cohomology of a scheme $X$ with values in a sheaf $F$ when a proper map $f: X \to Y$ is given. One has of course the Leray Spectral Sequence

$$H^p(Y, R^q f_* F) \Rightarrow H^{p+q}(X, F)$$

which "reduces" one to the problems of calculating

(a) the cohomology of sheaves on $Y$ and

(b) the higher direct images $R^q f_* F$.

Now for a proper map $f: X \to Y$ of paracompact spaces, one has the

result that the stalk of $R^q f_* F$ at a point $f$ of $Y$ is isomorphic to the cohomology $H^q(X_y, F/X_y)$ of the fibre [2]. This is false for the étale cohomology of schemes, but is true if one restricts to torsion sheaves:

Theorem (Grothendieck): Let $f: X \longrightarrow Y$ be a proper map, let $F$ be a torsion sheaf on $X$, let $\overline{y}$ be a geometric point of $Y$, and let $X_{\overline{y}}$ be the fibre of $X/Y$ at $\overline{y}$. Then the stalk

$$(R^q f_* F)_{\overline{y}} \approx H^q(X_{\overline{y}}, F/X_{\overline{y}}).$$

With this result, most questions for complete varieties can be reduced inductively to the case of dimension 1.

The theorem is obviously of a local nature on $Y$, and one can, by a limiting process, suppose that $Y$ is "local" for the étale topology, i.e., that $Y$ is the spectrum of a henselian ring with separably closed residue field and that $\overline{y}$ is the closed point of $Y$. Then the stalk of $R^q f_* F$ at $\overline{y}$ is just $H^q(X, F)$ and so the theorem reads

Same Theorem: With the notation as above, suppose $Y$ is the spectrum of a hensel ring with separably closed residue field and let $X_0$ be the closed fibre of $X/Y$. Then the natural map

$$H^q(X, F) \longrightarrow H^q(X_0, F|X_0)$$

is bijective for all $q$.

Outline of the proof:

Let's assume that $Y$ is noetherian and $X/Y$ is projective. So one can suppose $X$ is the projective space $\mathbb{P}^n_Y$. By projecting $\mathbb{P}^n \dashrightarrow \mathbb{P}^{n-1}$ and induction, one reduces to the case of relative dimension $\leq 1$ (in fact to the case $X = \mathbb{P}^1_Y$ if one wants). The case of relative dimension $\leq 1$ is the core of the proof.

We take the local version above. Now the cohomology group $H^q(X, F)$ is an effaceable functor of $F$, and it follows that to prove the isomorphism for each $F$ it suffices to prove bijectivity for $q = 0$ and only surjectivity for $q > 0$. That is an elementary exercise on morphisms of $\delta$-functors. Remember that we are in the case of relative dimension $\leq 1$, i.e., in the case $X_0$ is an algebraic scheme of dimension $\leq 1$. This is essentially the case of an algebraic curve, since nilpotents don't affect the étale topology, and is well under control. One knows that the cohomology of a torsion sheaf vanishes for $q > 2$. Hence surjectivity of the maps is trivial for $q > 2$ and it remains to prove

bijectivity for $q = 0$

surjectivity for $q = 1, 2$.

But one can do even better: If one is willing to vary $X$ as well as the sheaf one can reduce to the case $F = \mathbb{Z}/n$. This is done by untwisting a sheaf $F$ with the aid of the following

Lemma: Let $X$ be noetherian and $F$ a noetherian torsion sheaf on $X$. There is an integer $N$, a collection of finite morphisms $\pi_i : X_i' \longrightarrow X$, integers $n_i$, $i = 1, \ldots, N$, and an injection

$$0 \longrightarrow F \longrightarrow \prod_i \pi_{i*}(\mathbb{Z}/n_i).$$

In fact, with the lemma and induction, one reduces to the case $F = \pi_{i*}(\mathbb{Z}/n_i)$, and replacing $X$ by $X_i'$ to the case $F = \mathbb{Z}/n_i$.

Hence the proof is reduced to showing

$$H^q(X, \mathbb{Z}/n) \to H^q(X_0, \mathbb{Z}/n)$$

bijective if $q = 0$ and surjective if $q = 1, 2$. For $q = 0$, recall that of course $H^0(X, \mathbb{Z}/n) = (\mathbb{Z}/n)^c$ where $c$ is the number of connected

components of $X$ (assumed finite). Hence one has really to show that $X$ connected and nonempty implies $X_0$ connected and nonempty. This is an easy consequence of Hensel's lemma on $Y$. For $q = 2$, let us assume $n$ invertible on $Y$ so that we can replace $\mathbb{Z}/n$ by the (noncanonically) isomorphic sheaf $\mu_n$ and apply Kummer Theory. One finds a diagram

$$\begin{array}{ccccc} \text{Pic } X = H^1(X, \mathbb{G}_m) & \xrightarrow{a} & H^2(X, \mu_n) & & \\ \downarrow b & & \downarrow c & & \\ \text{Pic } X_0 = H^1(X_0, \mathbb{G}_m) & \xrightarrow{d} & H^2(X_0, \mu_n) & \longrightarrow & 0 \end{array}$$

where $d$ is surjective because $X_0$ is an (nonreduced) algebraic curve. Hence to show $c$ surjective it suffices to show $b$:

$$\text{Pic } X \longrightarrow \text{Pic } X_0$$

surjective. Again using Hensel's Lemma and the fact that $\dim X_0 \leqq 1$, it is easy to show that enough Cartier divisors on $X_0$ lift to $X$.

There remains the problem of $q = 1$. Now by general arguments, $H^1(X, \mathbb{Z}/n)$ classifies étale galois coverings of $X$ with galois group $\mathbb{Z}/n$. So the problem is to show that every galois covering of $X_0$ with group $\mathbb{Z}/n$ is induced by a covering of $X$. More generally, one has

Theorem (Grothendieck): Let $f: X \longrightarrow Y$ be proper with $Y$ henselian and let $X_0$ be the closed fibre of $X/Y$. Then every finite étale covering of $X_0$ is induced by a (unique) étale covering of $X$.

Unfortunately the proof is difficult.

## Bibliography

1. Artin, M., Grothendieck Topologies -- Lecture notes mimeographed at Harvard.

2. Godement, R., Topologie Algébrique et théorie des Faisceaux, Paris -- Hermann.

3. Ogg, A., Abelian Varieties over Function Fields, Annals, 1963.

4. Šafarevič, A russian paper.

5. Tate, J., unpublished.

# A DUALITY THEOREM IN THE ETALE COHOMOLOGY OF SCHEMES

J. L. Verdier

We shall present in this exposé a duality theorem which has been proved by A. Grothendieck. The formulation of this theorem is the same as those of the other duality theorems which can be found in nature: Duality for coherent sheaves [H.S.], duality in the cohomology of pro-finite groups, Poincaré's duality for topological varieties.... .

To get a duality theorem, we need a theory of cohomology with compact support (§ 2) . Then the duality is defined by the Gysin's morphism (or trace morphism) (§ 3) . In § 1 , we shall recall the base changing theorem for the étale cohomology which is the main instrument in this question.

## § 1. The base changing theorem in the étale cohomology of schemes.

Let us consider a cartesian square of preschemes:

$$\begin{array}{ccc} X & \xleftarrow{g'} & X' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ S & \xleftarrow{g} & S' \end{array}$$

and let $F$ be a torsion sheaf on $X$ for the étale topology. Let us suppose (to simplify) that the prescheme $S$ is locally noetherian. The obvious

natural transformation of functors:

$$f_* \longrightarrow g_* f'_* g'^*$$

(lower star = direct image, upper star = inverse image)

yields natural morphisms:

$$g^* R^q f_*(F) \longrightarrow R^q f'_* g^*(F)$$

1.1 THEOREM. (Artin-Grothendieck): The above morphisms are isomorphisms in the two following cases:

1) The morphism $f$ is <u>proper.</u>

2) The torsion of $F$ is prime to the residual characteristics of $S$.

The morphism $g$ is <u>smooth.</u>

§ 2. <u>The direct image functor with proper support.</u>

Let $f : X \longrightarrow S$ be a quasi-projective morphism of preschemes where $S$ is locally noetherian. Let $i: X \longrightarrow X'$ be an $S$-immersion of $X$ into a prescheme $X'$ projective on $S$. For any torsion sheaf on $X$ (for the étale topology), we shall denote by $R^q f_!(F)$ the sheaf on $S$:

$$R^q f_!(F) = R^q f'_*(i_!(F))$$

where $i_!(F)$ is the sheaf on $X'$ obtained by extending $F$ by zero and where $R^q f'_*$ is the $q$-th derived functor of the direct image by the morphism $f' : X' \longrightarrow S$.

When $S = \mathrm{spec}(\underline{C})$ (the field of complex numbers) and $X$ is a non-singular quasi-projective variety, the $R^q f_!$ are isomorphic to the cohomology groups with compact support of the corresponding topological variety. (Comparison theorem).

The sequence $R^q f_!$ ( $0 \leq q$) is a $\delta$-functor. It can be shown that it is in general <u>not</u> a derived functor.

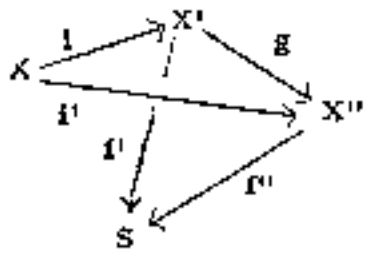
The $R^q f_!$ will be called the $\delta$-functor direct image with proper support. In order to give a sense to this definition we need the

2.1. PROPOSITION: The $\delta$-functor $R^q f_!$ does not depend on the immersion $i$ into a prescheme projective on $S$.

<u>Proof</u>: Let $i : X \longrightarrow X'$ and $i' : X \longrightarrow X''$ be two S-immersions. We shall only prove that there exists an isomorphism functorial in $F$:

$$R^q f'_*(i_!(F)) \xrightarrow{\sim} R^q f''_*(i'_!(F))$$

Making use of the fibered product, we can suppose that there exists an S-morphism $g: X' \longrightarrow X''$ such that the following diagram is commutative:




The composition spectral sequence gives:

$$R^p f'_* (R^q g_* (i_! F)) \Longrightarrow R^n f'_* (i_! F)$$

To determine the sheaf $R^q g_* (i_! (F))$, we can consider the fibers and apply the base changing theorem for a proper morphism. It becomes therefore clear that:

$$R^q g_* (i_! (F)) = 0 \qquad q > 0$$

and that the canonical morphism $i'_!(F) \longrightarrow g_* (i_! (F))$ is an isomorphism. What remains to be shown is that those various isomorphisms are compatible. This can be done by the same methods.

The properties of the functor $R^q f_!$ are summed up in the following

2.2. PROPOSITION: 1) The functor $R^q f_!$ commutes with the change of the base.

1)' When $f$ is quasi-finite, $R^q f_! = 0$ $(q \neq 0)$. In particular when $f$ is étale $R^q f_! = 0$ $(q \neq 0)$ and $f_!$ is thefunctor extension by zero.

2) We have a spectral sequence of composition.

3) Let $Y \hookrightarrow X$ be a closed sub-prescheme and $U$ the complementary open sub-prescheme. Let $F_{U!}$ be the sheaf restricted to $U$ and extended by zero on $X$ and $F_Y$ be the direct image on $X$ of the restriction of $F$ on $Y$.

We get an unrestricted exact sequence:

$$\ldots \longrightarrow R^q f_!(F_{U'}) \longrightarrow R^q f_!(F) \longrightarrow R^q f_!(F_Y) \longrightarrow R^{q+1} f_!(F_{U'}) \longrightarrow \ldots$$

4) Let $(U_\alpha \longrightarrow X)$ be a separated étale covering of $X$. For any simplex $\sigma = (\alpha_1, \alpha_2, \ldots, \alpha_p)$ we shall denote by $U_\sigma$ the prescheme $U_{\alpha_1} \times_S \ldots \times_S U_{\alpha_p}$ and by $f_{U_\sigma}$ the morphism $f$ composed with the canonical morphism $U_\sigma \longrightarrow X$. Let us denote by $F/U_\sigma$ the inverse image of the sheaf $F$ on $U_\sigma$. For any $q \geq 0$ and for any simplicial application $\sigma \longrightarrow \sigma'$, we get a morphism of sheaves on $S$:

$$R^q f_{U_\sigma !}(F/U_\sigma) \longrightarrow R^q f_{U_{\sigma'} !}(F/U_{\sigma'})$$

which yields a semi-simplicial complex

$$\cdots \rightrightarrows \coprod_{\alpha,\beta} R^q f_{U_\alpha \times_S U_\beta !}(F/U_\alpha \times_S U_\beta) \rightrightarrows \coprod_{\alpha} R^q f_{U_\alpha !}(F/U_\alpha)$$

Let us denote by $H_p(R^q f_{\mathcal{U}!}, F)$ the $p$-th homology sheaf of the above complex.

If the covering is <u>finite</u> or if the dimension of the fibers of the morphism $f$ is <u>bounded</u>, we get a spectral sequence:

$$E_2^{p,q} = H_{-p}(R^q f_{\mathcal{U}!}, F) \Longrightarrow R^* f_!(F) \quad .$$

When the fibers of the morphism $f$ are of dimension $\leq d$, the above spectral sequence yields the exact sequence:

$$(2.2.1) \quad \coprod_{\alpha,\beta} R^{2d} f_{U_\alpha \times_S U_\beta !}(F/U_\alpha \times_S U_\beta) \rightrightarrows \coprod_{\alpha} R^{2d} f_{U_\alpha !}(F/U_\alpha) \longrightarrow R^{2d} f_!(F) -$$

Proof: The first three assertions are obvious. Let us prove the fourth one. Let us denote by $F_{U\sigma!}$ the sheaf restricted to $U_\sigma$ and extended by zero. The complex of sheaves on X: $C^*(U_\alpha, F)$ deduced from the semi-simplicial complex

$$\rightrightarrows \coprod_{\alpha,\beta} F_{U_\alpha \times_S U_\beta !} \rightrightarrows \coprod_{\alpha} F_{U_\alpha !} \longrightarrow F$$

is acyclic (look at the fibers). Taking an immersion $i : X \longrightarrow X'$ into a projective prescheme over S, we can take a resolution of the complex $i_! C^*(U, F)$ by object which are $f'_*$-acyclic ($f'$: $X' \longrightarrow S$). The spectral sequence of the double complex obtained by applying the functor $f'_*$ yields the expected result.

§ 3. The trace morphism.

In this paragraph, we are mainly interested in the morphisms $f : X \longrightarrow S$ of preschemes which possess the following property:

(S) f is a smooth and quasi-projective morphism. The prescheme S is locally noetherian. The dimension d of the fiber at any point $x \in X$ is independent of the considered point.

The number d will be called the relative dimension of X over S.

The sheaf $\mu_n$ (n prime to the residual characteristics of S) is defined by the exact sequence :

$$(3.0.1) \qquad 0 \longrightarrow \mu_n \longrightarrow \underline{G}_m \xrightarrow{n} \underline{G}_m \longrightarrow 0$$

($\underline{G}_m$ denotes the sheaf: multiplicative group)

The sheaf on $X$ : $\mu_n^d$ will play the role of a relative orientation sheaf of $X$ over $S$ and will be denoted by $T_{X/S}$. The sheaf $T_{X/S}$ is stable by the change of the base.

Let $S = \mathrm{spec}(k)$, $k$ an algebriacally closed field, and $X$ be a complete connected non-singular curve over $S$. The exact sequence (3.0.1) yields the exact sequence of abelian groups:

$$(3.0.2.) \qquad 0 \longrightarrow H^0(X,\mu_n) \longrightarrow H^0(X,\underline{G}_m) \xrightarrow{n} H^0(X,\underline{G}_m) \longrightarrow$$

$$H^1(X,\mu_n) \longrightarrow H^1(X,\underline{G}_m) \xrightarrow{n} H^1(X,\underline{G}_m) \longrightarrow H^2(X,\mu_n) \longrightarrow 0 .$$

Since the field $k$ is algebraically closed, $X$ is complete, and $n$ prime to the characteristic of $k$, the morphism $H^0(X,\underline{G}_m) \xrightarrow{n} H^0(X,\underline{G}_m)$ is surjective. Since furthermore the group $H^1(X,\underline{G}_m)$ is isomorphic to the Picard's group of $X$, the sequence (3.0.2) yields two cononical isomorphis

$$H^1(X,\mu_n) \xrightarrow{\sim} J_n(X)$$

the points of order $n$ of the jacobian variety of $X$, and

$$(3.0.3) \qquad \zeta_X : H^2(X,\mu_n) \xrightarrow{\sim} \underline{Z}/n$$

Let us suppose now that $X = A_k^1 = \mathrm{spec}(k[t])$, ($k$ algebraically closed field) and let $f: X \longrightarrow S = \mathrm{spec}(k)$ the canonical morphism. The canonical immersion $i : A_k^1 \longrightarrow P_k^1$ (projective space of dimension 1 ov k) yields the exact sequence of sheaves on $P_k^1$ :

$$0 \longrightarrow \mu_{n_{X!}} \longrightarrow \mu_n \longrightarrow \mu_{n_\infty} \longrightarrow 0$$

Since $\mu_{n_\infty}$ is obviously an acyclic sheaf over $P^1_k$, we get a sequence of isomorphisms:

$$R^2f_!(\mu_n) \xrightarrow{\sim} H^2(P^1_k, \mu_{n_{X!}} \xrightarrow{\sim} H^2(P^1_k, \mu_n) \xrightarrow{\sim} \underline{Z}/n$$

Let us denote by:

(3.0.4) $$\omega_k : R^2f_!(\mu_n) \xrightarrow{\sim} \underline{Z}/n$$

the composed isomorphism. We can now formulate the main proposition of this paragraph. (From now on, except when explicitly mentioned, the sheaves considered will be sheaves of $\underline{Z}/n$-modules.

3.1. PROPOSITION: It is possible in only one manner to attach to any morphism $f : X \longrightarrow S$ satisfying (S), and to any sheaf $F$ on $S$, one morphism (called the trace morphism) :

$$\rho_{X,S}(F) : R^{2d}f_!(f^*(F) \otimes T_{X/S}) \longrightarrow F$$

(d is the relative dimension of $X$ over $S$) such that:

TR0) $\rho_{X,S}(F)$ is functorial in $F$.

TR1) $\rho_{X,S}$ is compatible with the change of the base.

TR2) $\rho_{X,S}$ is compatible with the composition of the morphisms.

TR3) When $f$ is étale, $\rho_{X,S}$ is the canonical morphism yielded by the adjunction formula.

TR4) When $S = \mathrm{spec}(k)$, $X = A^1_k$, $F = \underline{Z}/n$, the morphism $\rho_{X,S}(\underline{Z}/n)$ is equal to $\omega_k$ (3.0.4).

Furthermore the morphism $\rho_{X,S}$ possesses the following properties:

(a) When the fibers of the morphism $f$ are connected and non-empty, $\rho_{X,S}$ is an isomorphism.

(b) When $S = \mathrm{spec}(k)$ ($k$ algebraically closed field), when $X$ is a complete, connected, non-singular curve and when $F$ is $\underline{Z}/n$, the morphism $\rho_{X,S}$ is equal to $\eta_X$ (3.0.3).

(c) The morphisms $\rho_{X,S}$ for different $n$ are compatible.

Let us first elucidate the axiom (TR2). Let $f : X \longrightarrow S$ and $g : S \longrightarrow Y$ be two morphisms of preschemes satisfying (S). Let $d$ and $d'$ be the respective relative dimensions. The functor $R^q f_!$ (resp. $R^q g_!$) is null for $q > 2d$ (resp. $q > 2d'$). Therefore the spectral sequence of composition yields an isomorphism

$$R^{2d'}g_! R^{2d}f_! \xrightarrow{\sim} R^{2(d-d')}gf_! \ .$$

Furthermore the orientation sheaf $T_{X/Y}$ is canonically isomorphic to $T_{X/Y} \otimes f^*(T_{S/Y})$ so that we have, for any sheaf $F$ on $Y$, a natural isomorphism $\alpha$ that we can include in a diagram :

(3.1.1)

$$\begin{array}{ccc}
R^{2(d+d')}gf_!(T_{X/S} \otimes f^*g^*F) & \xrightarrow[\alpha]{\sim} & R^{2d'}g_! R^{2d}f_!(T_{X/S} \otimes f^*(T_{S/Y} \otimes g^*F)) \\
\Big\downarrow{\scriptstyle \rho_{X,Y}} & & \Big\downarrow{\scriptstyle R^{2d'}g_!(\rho_{X,S})} \\
F & \xleftarrow{\rho_{Y/S}} & R^{2d'}g_!(T_{S/Y} \otimes g^*F)
\end{array}$$

The axiom (TR2) is that the above diagram must be commutative.

Proof of the proposition: Uniqueness: By (TR1) we are reduced to the case $S = \mathrm{spec}(k)$ where $k$ is an algebraically closed field. By (TR2), (TR3) and the exact sequence (2, 2, 1) we are reduced to the case when $X$ is affine and $f$ of the type:

$$X \xrightarrow{g} \underline{A}^d_k \longrightarrow \mathrm{spec}(k)$$

where $g$ is étale and $\underline{A}^d_k$ is the affine space of dimension $d$ over $k$ (Definition of smooth morphism). By (TR3) and (TR2) we are reduced to the case $X = \underline{A}^d_k$ and $f : \underline{A}^d_k \longrightarrow \mathrm{spec}(k)$ the canonical morphism. By induction on $d$ and (TR2) we are reduced to the case $f : \underline{A}^1_k \longrightarrow \mathrm{spec}(k)$. Since the functors $R^q f_!$ commute with inductive limits we can suppose that $F = \underline{Z}/n$. The axiom (TR4) completes the proof.

Existence: We shall sketch the main steps of the proof.

(1) Suppose that the morphism $\rho_{X,S}$ is constructed when $S$ and $X$ are affine and when $f$ is of the type $X \xrightarrow{g} \underline{A}^d_S \longrightarrow S$ with $g$ étale and that it satisfies (TR1), $0 \leq i \leq 4$. Then, by localization on $X$ (2, 2, 1) and on $S$, we can construct it in the general case. The properties (TR1), $0 \leq i \leq 4$, can easily be verified.

(2) There exists one and only one functorial isomorphism:

$$R^{2d} f_!(T_{X/S} \otimes f^*F) \longrightarrow R^{2d} f_!(T_{X/S}) \otimes F$$

such that the properties (TR1) and (TR2) are satisfied, so that all we have to do is to construct the morphism $\rho_{X,S}$ only when $F$ is the constant sheaf $\underline{Z}/n$.

(3) Suppose that the morphism $\rho_{X,S}$ is constructed in the two following cases:

(1) The morphism f is étale and the morphism $\rho_{X,S}$ possesses the properties (TR1), (TR2), and (TR3).

(2) The morphism f is the canonical morphism $\underline{A}^d_S \longrightarrow S$ and the morphism $\rho_{X,S}$ possesses the properties (TR1), (TR4) and the property:

(TR2)' The morphism $\rho_{X,S}$ is compatible with the S-automorphisms of $\underline{A}^d_S$ induced by the permutations of the indeterminates.

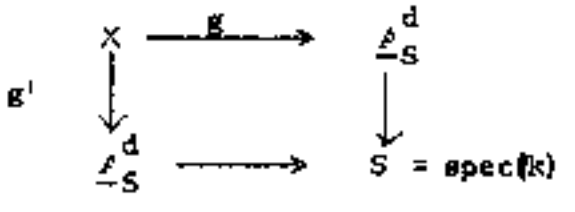
Suppose furthermore that the thus constructed morphisms verify the following compatibility property:

(C) For any diagram:

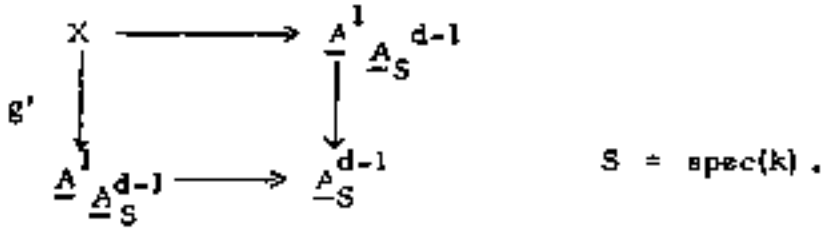
$$\begin{array}{ccc} X & \xrightarrow{g'} & \underline{A}^1_k \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h'} \\ \underline{A}^1_k & \xrightarrow{h'} & S = \mathrm{spec}(k) \end{array}$$

with g and g' étale and h and h' canonical, the two morphisms $R^2f_!(T_{X/S}) \longrightarrow \underline{Z}/n$ obtained by applying (3.1.1) are equal. Then we can construct $\rho_{X,S}$ in the general case.

Let us prove this assertion. Let $f : X \xrightarrow{g} \underline{A}^d_S \longrightarrow S$ be a morphism with g étale. We shall define $\rho_{X,S}$ by the diagram (3.1.1). The only point to be shown is that the so constructed morphism does not depend on the factorization of f. The properties (TR4) can be easily deduced afterward. To show this independence, we can suppose that S = spec(k) (algebraically closed field). Let us consider




two factorizations of $f$. An $S$-morphism of $X$ into an affine space over $S$ is determined by $d$ global sections of $0_X$ : $\eta_1, \eta_2, \ldots \eta_d$. Let $\Omega_{X/S}$ be the coherent sheaf of the relative differentials of $X$ on $S$. The sheaf $\Omega_{X/S}$ is locally free of rank $d$ on $0_X$. Let $d\eta_1 \ldots d\eta_d$ be the differentials of the sections $\eta_1 \ldots \eta_d$. The conditions for the morphism $g$ to be étale are that the sections $d\eta_i$ of $\Omega_{X/S}$ generate the sheaf $\Omega_{X/S}$. Let $\eta'_1, \ldots \eta'_d$ be $d$ sections of $0_X$ which determine the morphism $g'$. The question being local on $X$, we can see easily, through permutations of the variables and successive substitutions, that we are reduced to the case $\eta'_i = \eta_i$, $2 \leq i \leq d$. That means that the following diagram is commutative:




But now looking at the fibers on $\underline{A}^{d-1}_S$ and applying the property (C) we are done.

(4) Let us define the morphism $\rho_{X,S}$ for $f$ étale in the obvious way. The properties (TR1), (TR2), (TR3) can easily be verified. For $f : \underline{A}^d_S \longrightarrow S$ we shall define $\rho_{X,S}$ by induction on $d$ so that we are reduced to the case $d = 1$. Using arguments similar to those used in the beginning of this paragraph, all that is left for us to do is to define the morphism $\rho_{X,S}$ when $X = \underline{P}^1_S$. But in this case the sheaf on $S$ :

$R^1f_!(G_m)$ is canonically isomorphic to the constant sheaf $\underline{Z}$ and the construction is easy. The properties (TR1), (TR2)' and (TR4) are obvious so that we still have to check the property (C). This can be done by classical arguments using the norm.

To achieve the proof, we have to check the properties (a), (b), and (c). The properties (b) and (c) are obvious. To check the property (c) we are immediately reduced to the case $S = spec(k)$ (algebraically closed field). Then we can use the nice neighborhoods of M. Artin and proceed by induction.

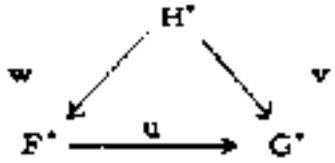
## § 4. Formulation of the duality theorem.

In this paragraph the morphism $f: X \longrightarrow S$ of preschemes with the property (S) will be fixed once for all. The relative dimension of $X$ over $S$ is $d$.

4.1 The derived category: We shall denote by $D_n(X)$ (resp. $D_n(S)$) the derived category of the abelian category of sheaves of $\underline{Z}/n$-modules on $X$ (resp. $S$) [H.S.]. Let us recall briefly what this category is. $D_n(X)$ is the category of complexes $F^*$ of sheaves (the differential is of degree $+1$), up to homotopy in which the morphisms which induce isomorphisms on the objects of cohomology are inverse.

The category $D_n^+(X)$ (resp. $D_n^-(X)$, resp. $D_n^b(X)$) is the full subcategory of the complexes $F^*$ of $D_n(X)$ whose objects $(F^*)^\ell$ are null for $\ell < \ell^0(F^*)$ (resp. $\ell > \ell^0(F^*)$, resp. $\ell^0(F^*) < \ell$ and $\ell < \ell^1(F^*)$).

The category $D_n(X)$ possesses a triangulated structure, i.e., for any morphism $F^\cdot \xrightarrow{u} G^\cdot$ we get a triangle that is unique up to non-unique isomorphism (the mapping cylinder):

$\deg(w) = 1$  (*)



Such triangles are called the distinguished triangles.

A functor $D_n(X) \longrightarrow D_n(S)$ is exact if it transforms distinguished triangles into distinguished triangles.

A cohomological functor R from $D_n(X)$ into an abelian category transforms any distinguished triangle (*) into an infinite exact sequence:

$$\ldots \longrightarrow R^0F^\cdot \longrightarrow R^0G^\cdot \longrightarrow R^0H^\cdot \longrightarrow R^1F^\cdot \longrightarrow \ldots$$

The usual functor "cohomology" is a cohomological functor with values in the category of sheaves on X.

The functor $\mathrm{Hom}_{D_n(\mathbb{Z})}(F^\cdot, .)$ (resp. $\mathrm{Hom}_{D_n(X)}(. , F^\cdot)$) is a cohomological functor (resp. a contravariant cohomological funcotr). The group $\mathrm{Hom}_{D_n(X)}(F^\cdot, G^\cdot)$ is sometimes called the hyper-$\mathrm{Ext}^0$ group.

The category $D_n^+(X)$ is equivalent to the category of complexes of injective sheaves, bounded below, up to homotopy. A resolution $F^\cdot \longrightarrow G^\cdot$ of a complex $F^\cdot$ is a morphism which induces isomorphisms on the cohomology, i.e., which yields an isomorphism in the category $D_n(X)$.

To any sheaf $F$ on $X$ we shall associate the following complex of sheaves on $X$ also denoted by $F$ :

$$(F)^{\ell} = 0 \quad \text{for } \ell \neq 0$$

$$(F)^{0} = F$$

$$d^{\ell} = 0$$

The functor thus defined from the sheaves on $X$ into $D_n(X)$ is fully faithful. Exact sequences of sheaves on $X$ yeilld functorially distinguished triangles.

4.2. The exact functor $Rf_!$ .

Let $X \xrightarrow{i} X' \xrightarrow{f} S$ be an S-imersion of $X$ into a projective prescheme over S. Let $F^{\cdot}$ be a complex of sheaves on $X$ bounded below and let us take a resolution of $i_!F^{\cdot}$ by a complex of injective sheaves on $X'$ . Applying the functor $f_*$ we get a complex of sheaves on $S$ and therefore an object of $D_n(S)$ which we shall denote by $\underline{R}f_!(F^{\cdot})$ . It can be shown that the object $\underline{R}f_!(F^{\cdot})$ depends functorially on $F^{\cdot}$ , (it does not depend up to unique isomorphism on the injective resolution and on the immersion $i$ , prop. 2.1). Furthermore the functor $\underline{R}f_!$ can be uniquely factorized through the category $D_n^+(X)$. The functor thus defined will be again denoted by:

$$\underline{R}f_! : D_n^+(X) \longrightarrow D_n^+(S) \ .$$

The functor $\underline{R}f_!$ is exact. For any sheaf $F$ on $X$ the cohomology sheaves of the complex $\underline{R}f_!(F)$ are isomorphic to the sheaves $R^q f_!(F)$ , (cf. § 2).

Since the functor $f'_*$ is of finite cohomological dimension (2d), the functor $\underline{R}f_!$ can be extended to the categories $D_n(X) \longrightarrow D_n(S)$ (we can take a resolution of any complex on $X'$ by complexes whose objects are $f'_*$ -acyclic) and by restriction to sub-categories yields various functors:

$$\underline{R}f_! : D_n^-(X) \longrightarrow D_n^-(S)$$

$$\underline{R}f_! : D_n^b(X) \longrightarrow D_n^b(S)$$

4.3 PROPOSITION. 1) Let $S \xrightarrow{g} Y$ be another morphism of prescheme possessing the property (S). The canonical morphism $\underline{R}(gf)_! \longrightarrow \underline{R}g_!\underline{R}f_!$ is an isomorphism.

2) Consider the following cartesian square:

$$\begin{array}{ccc} X & \xleftarrow{u} & X' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ S & \xleftarrow{u'} & S' \end{array}$$

The canonical morphism of functors:

$$u'^*\underline{R}f_! \longrightarrow \underline{R}f'_!u^*$$

is an isomorphism.

The first assertion is obvious, the second one is the base changing theorem for proper morphism.

4.4. The twisted inverse image functor.

Let $G = \ldots \longrightarrow G^{\ell} \xrightarrow{d^{\ell}} G \longrightarrow G^{\ell+1} \longrightarrow \ldots$ be a complex of sheaves on S. We shall denote by $f^!(G')$ the following complex of sheaves on X :

$$(f^!(G'))^{\ell} = f^*(G^{\ell+2d}) \otimes T_{X/S}$$

$$d^{\ell}(f^!(G')) = f^*(d^{\ell+2d}) \otimes id_{T_{X/S}}$$

This functor obviously yields an exact functor also denoted by $f^!$ :

$$f^! : D_n(S) \longrightarrow D_n(X)$$

By restriction, this functor yields various functors:

$$D_n^+(S) \longrightarrow D_n^+(X)$$

$$D_n^-(S) \longrightarrow D_n^-(X)$$

$$D_n^b(S) \longrightarrow D_n^b(X)$$

4.5 PROPOSITION: 1) Let $S \xrightarrow{g} Y$ be another morphism of preschemes with the property (S). The canonical morphism $gf^! \longrightarrow f^!g^!$ is an isomorphism

2) Consider the following cartesian square:

$$\begin{array}{ccc} X & \xleftarrow{u} & X' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ S & \xleftarrow{u'} & S' \end{array}$$

The canonical morphism $f'^{!}u'^{*} \longleftarrow u^{*}f^{!}$ is an isomorphism.

Those two assertions are obvious.

4.6 The trace morphism in the derived categories.

Let $X \xrightarrow{i} X' \xrightarrow{f'} S$ be an S-immersion of $X$ into a projective prescheme over $S$, and $G$ be a sheaf on $S$. Let us take now a resolution on $X'$ of the complex $i_!f^{!}(G)$ :

$$0 \longrightarrow 0 \longrightarrow I^{-2d} \longrightarrow I^{-2d+1} \longrightarrow \ldots \longrightarrow I^{0} \xrightarrow{d^{0}} I^{1} \longrightarrow \ldots$$

Let $Z^{0}$ be the kernel of the morphism $d^{0}$. We have a resolution

$$C^{*}(G) = \ldots\ 0 \longrightarrow I^{-2d} \longrightarrow I^{-2d+1} \longrightarrow \ldots \longrightarrow I^{-1} \longrightarrow Z^{0} \longrightarrow 0 \longrightarrow$$

of $i_!f^{!}(G)$ by $f'_*$-acyclic objects and therefore the complex on $S$ : $f'_*(C^{*}(G))$ is canonically isomorphic in $D_n(S)$ to the complex $\underline{R}f_!f^{!}(G)$. But now it is clear that we have a canonical morphism of complexes:

$$\underline{R}f_!f^{!}(G) \longrightarrow R^{2d}f_!(f^{*}(G) \otimes T_{X/S})$$

and using the trace morphism we get a functorial morphism:

$$Tr_{X/S} : \underline{R}f_!f^{!}(G) \longrightarrow G$$

This morphism can easily be extended (by means of Cartan-Eilenberg resolutions) to any complex of sheaves on $S$, and yields a morphism of exact functors.

4.7 The duality morphism:

Let $K^\cdot$ be an object of $D_n^+(X)$ and $H^\cdot$ be an object of $D_n(X)$. Let us denote by $\underline{R}\mathrm{Hom}(H^\cdot, K^\cdot)$, the following complex on $X$: Take an injective resolution $I^\cdot$ of the complex $K^\cdot$ and consider the object of $D_n(X)$ defined by the complex of sheaves: $\underline{\mathrm{Hom}}^*(H^\cdot, I^\cdot)$ where $\underline{\mathrm{Hom}}$ is the homomorphism sheaf. Let us assume now that $H^\cdot$ is an object of $D_n^-(X)$ and let us apply the functor global section on $X$. We get now an object of $D(Ab)$ which we shall denote by : $\underline{R}\mathrm{Hom}(H^\cdot, K^\cdot)$. The sheaves of cohomology of $\underline{R}\mathrm{Hom}(H^\cdot, K^\cdot)$ are the local hyper-ext. The groups of cohomology of $\underline{R}\mathrm{Hom}(H^\cdot, K^\cdot)$ are the global hyper-ext.

In the same way we define $\underline{Rf}_*(K^\cdot)$ : Take an injective resolution and apply the direct image functor.

By functoriality of $Rf_!$, for any $H^\cdot$ object of $D_n^-(X)$ and $K^\cdot$ object of $D_n^+(X)$, we get a functorial morphism:

$$\underline{Rf}_*\underline{R}\mathrm{Hom}(H^\cdot, K^\cdot) \longrightarrow \underline{R}\mathrm{Hom}(Rf_!(H^\cdot), Rf_!(K^\cdot))$$

which gives, when we apply the functor global section on $S$, a functorial morphism:

$$\underline{R}\mathrm{Hom}(H^\cdot, K^\cdot) \longrightarrow \underline{R}\mathrm{Hom}(\underline{Rf}_!(H^\cdot), \underline{Rf}_!(K^\cdot))$$

which yields, taking the cohomology, functorial morphism of groups :

$$\mathrm{Ext}^p(H^\cdot, K^\cdot) \longrightarrow \mathrm{Ext}^p(\underline{Rf}_!(H^\cdot), \underline{Rf}_!(K^\cdot))$$

But now using the trace morphism, we obtain morphisms:

$$\Delta^1_{X/S} : \underline{Rf}_!\underline{RHom}(F^\cdot, f^!G^\cdot) \longrightarrow \underline{RHom}(\underline{Rf}_!F^\cdot, G^\cdot)$$

$$\Delta^2_{X/S} : \underline{RHom}(F^\cdot, f^!G^\cdot) \longrightarrow \underline{RHom}(\underline{Rf}_!F^\cdot, G^\cdot)$$

$$\Delta^3_{X/S} : Ext^p(F^\cdot, f^!G^\cdot) \longrightarrow Ext^p(\underline{Rf}_!F^\cdot, G^\cdot)$$

for any $F^\cdot$ object of $D_n^-(X)$ and $G^\cdot$ object of $D_n^+(S)$.

Let us then formulate the duality theorem:

4.8 THEOREM (A. Grothendieck): The morphisms $\Delta^i_{X/S}$ $(i = 1, 2, 3)$ are isomorphisms.

REMARK 1: Assume $S = spec(k)$ (algebraically closed field) and $X$ connected. Let $G^\cdot$ be the group $\underline{Z}/n$ and $F^\cdot = F$ be a sheaf on $X$. The duality theorem yields an isomorphism (we shall denote by $H^p_c(X, F)$ the groups $R^pf_!(F)$):

$$Hom(H^p_c(X, F), \underline{Z}/n) \xrightarrow{\sim} Ext^{2d-p}(X, F, T_{X/S})$$

Assume furthermore that $F$ is locally free and of finite type. Using spectral sequence from local Ext to global Ext we obtain: ($F' = Hom(F, T_{X/S})$)

$$Hom(H^p_c(X, F), \underline{Z}/n) \xrightarrow{\sim} H^{2d-p}(X, F')$$

which can also be formulated in the following way: The cup-product

$$H^p_c(X, F) \otimes H^{2d-p}(X, F') \longrightarrow H^{2d}_c(X, T_{X/S}) \xrightarrow{\sim} \underline{Z}/n$$

is a perfect duality. This is one of the classical formulations of the theorem of Poincaré.

REMARK 2: Using localization (associated sheaf) and global section (spectral sequence from local to global), it is easy to see that if for some $i$ ($i = 1, 2, 3$) the morphism $\Delta^i_{X/S}$ is always an isomorphism, all the $\Delta^i_{X/S}$ are isomorphisms.

§ 5. Proof of the duality theorem.

We shall sketch the proof of the duality theorem.

Let us recall first that, the preschemes $X$ and $S$ being locally noetherian, the categories of sheaves on $X$ and $S$ are locally noetherian. Let us recall also that a noetherian sheaf $G$ is constructible, i.e., any point possesses a neighborhood which possesses a finite partition into locally closed subsets on which the sheaf $G$ is locally constant and of finite type. In particular any constructible sheaf is locally constant in the neighborhood of the generic point of any irreducible component. It can be shown (as a corollary to the base changing theorem for proper morphism) that the direct images (including the $q$-th direct images $q \neq 0$) of a constructible sheaf by a proper morphism are constructible.

Let $X \xrightarrow{f} S$ be a morphism which possesses the property (S), $F^*$ be an object of $D^-_n(X)$ and $G^*$ be an object of $D^+_n(S)$. We shall denote by $(i, X, S, F^*, G^*)$ the property: The morphism $\Delta^i_{X/S}(F^*, G^*)$ is an isomorphism.

5.1 LEMMA: The following properties are equivalent:

(i) The duality theorem is true for the morphism f,

(ii) There exists an i(i = 1, 2, 3) and an étale covering $(U_j \longrightarrow X)$ such that, for any quasi-projective étale morphism $U \longrightarrow X$ which can be factorized by the above covering and for any constructible sheaf G on S we have the property $(i, X, S, \underline{Z}/n_{U_j}, G)$.

5.2 LEMMA: The duality theorem is true when f is étale.

5.3 LEMMA: Let $S \xrightarrow{g} Y$ be a morphism with the property (S), $H^*$ an object of $D_n^+(Y)$ and i be an integer $0 < i \leq 3$. Let us suppose that two of the properties below hold:

$$(i, X, S, F^*, g^!H^*) \qquad (i, X, Y, F^*, H^*) \qquad (i, S, Y, Rf_!F^*, H^*)$$

Then the third one also holds.

Proof: The last lemma comes directly from the transitivity property (4.3; 4.5; 3.1 (TR2)). The second one is obvious. Let us prove the first one. Any object $F^*$ of $D_n^-(X)$ admits a resolution $P^* \longrightarrow F^*$ by a complex of the type : $P^* = \ldots \longrightarrow \underline{Z}/n_{U_j}! \longrightarrow \underline{Z}/n_{U_k}! \longrightarrow 0 \longrightarrow \ldots$ where the $U_i$ and the $U_k$ are étale over X and can be factorized by the covering $(U_j \longrightarrow X)$. So that, by spectral sequence argument or by the way out functor lemma [H, S, ] in order to prove the duality theorem, we are brought back to the case $F^* = \coprod_i \underline{Z}/n_{U_i}!$, with $U_i$ noetherian.

Since the functors $R^q f_!$ and $Ext^p$ commute with the infinite sum we are brought back to the case $F^* = \underline{Z}/n_{U_i!}$. Again by spectral sequence argument we can suppose that $G^* = G$ is one sheaf over $S$. But now, since the sheaves $\underline{Z}/n_{U_i!}$ and $R^q f_!(\underline{Z}/n_{U_i!})$ are noetherian sheaves, the hyper-ext $Ext^*(\underline{R}f_!(\underline{Z}/n_{U_i!}), G)$ and $Ext^*(\underline{Z}/n_{U_i!}, f^!G)$ commute with the direct limit of $G$ and therefore we can suppose that $G$ is noetherian, i.e., constructible. We thus prove the implication (ii) $\Longrightarrow$ (i). The other implication is obvious.

5.4 First reduction: Using the three lemmas above and straight forward arguments we are brought back to the proof of the theorem in the following case:

(a) The morphism $f : X \longrightarrow S$ is of relative dimension 1. $X$ and $S$ are affine noetherian.

(b) The complex $F^*$ is the constant sheaf $\underline{Z}/n$.

(c) The complex $G^*$ is a constructible sheaf.

Thus, by the first reduction, we have to check that the morphism

$$(5.4.1)\quad \triangle^1_{X/S} : \underline{R}f_*(f^!G) \longrightarrow \underline{RHom}(\underline{R}f_!(\underline{Z}/n), G)$$

is an isomorphism.

Let $\eta \in S$ be a generic point of an irreducible component of $S$. The sheaves $G$ and $R^q f_!(\underline{Z}/n)$ are constant on an étale neighborhood of $\eta$ (they are constructible). Therefore the cohomology sheaves of the complex $\underline{RHom}(\underline{R}f_!(\underline{Z}/n), G)$ are constant on an étale neighborhood

of $\eta$.

5.5 LEMMA: Assume conditions (a), (b), (c) of the reduction 5.4. Denote by $\bar{\eta}$ a geometric fiber of $f$. The cohomology sheaves of $\underline{R}f_*(f^!G)$ are constant on an étale neighborhood of $\eta$. The complex $\underline{R}f_*(f^!G)_{\bar{\eta}}$ is canonically isomorphic (in $D_n(Ab)$) to the complex $\underline{R}f_{\bar{\eta}*}(f_{\bar{\eta}}^! G_{\bar{\eta}})$.

We shall not prove this lemma. It follows from the "relative purity theorem" [S.G.A.A.], which is one of the consequences of 1.1.

But now, by the lemma 5.5, to see that the morphism (5.4.1) is an isomorphism on a neighborhood of $\eta$, it is enough to look at the fiber $X_{\bar{\eta}} \longrightarrow \bar{\eta}$, i.e., we are reduced to the case $S = spec(k)$ (k an algebraically closed field). Furthermore, to prove that (5.4.1) is an isomorphism we are reduced, by an easy noetherian induction on the support of the sheaf $G$, to the case where the support of $G$ is a closed point of $S$, and we are immediately reduced again to the case $S = spec(k)$ (algebraically closed field).

Let us suppose that $S = spec(k)$, we can embed the curve $X$ into a complete non-singular curve $X'$ and we are easily reduced to prove the duality theorem in the case

(a)' $X \longrightarrow S$ is a complete non-singular curve over an algebraically closed field.

(b)' The complex $F'$ is the constant sheaf $\underline{Z}/n$.

(c)' The complex $G'$ is the constant sheaf $\underline{Z}/n$.

Thus we have to prove that the morphisms:

$$H^0(X, \mu_n) \longrightarrow \mathrm{Hom}(H^2(X, \underline{Z}/n), \underline{Z}/n) \qquad (5.5.1)$$

$$H^1(X, \mu_n) \longrightarrow \mathrm{Hom}(H^1(X, \underline{Z}/n), \underline{Z}/n) \qquad (5.5.2)$$

$$H^2(X, \mu_n) \longrightarrow \mathrm{Hom}(H^0(X, \underline{Z}/n), \underline{Z}/n) \qquad (5.5.3)$$

are isomorphisms. This can be seen easily for (5.5.1) and (5.5.3). For (5.5.2) this follows from the autoduality of the jacobian variety of $X$.

## BIBLIOGRAPHY

[S.G.A.A.] Séminaire de Géométrie Algébrique de l'Institut des Hautes Etudes Scientifiques by M. Artin and A. Grothendieck. (1964).

[G.T.] Grothendieck topologies: Notes on a seminar by M. Artin, 1962, Harvard University.

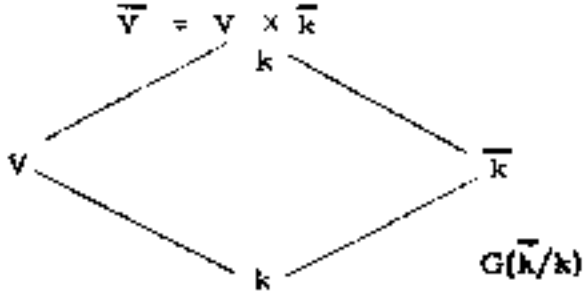
[H.S.] Hartshorne Seminar, (1964), Harvard University.

# ALGEBRAIC COHOMOLOGY CLASSES

J. Tate

The $\ell$-adic étale cohomology of algebraic varieties is much richer than the classical cohomology in that Galois groups operate on it. This opens up a new field of inquiry, even in the classical case. Although theorems seem scarce, the soil is fertile for conjectures. I ask your indulgence while I discuss some of these, together with some meager evidence, both computational and philosophical, for them. The main idea is, roughly speaking, that a cohomology class which is fixed under the Galois group should be algebraic when the ground field is finitely generated over the prime field. I have come to this idea by way of its relation to questions of orders of poles of zeta functions. Most of the signposts along the way became visible to me during conversations and/or correspondence with M. Artin, Mumford, and Serre. I thank them heartily for their guidance.

§1. The $\ell$-adic cohomology. Throughout our discussion we shall consider the situation pictured below, in which $k$ is a field, $\bar{k}$ an




algebraically closed extension field, $G(\bar{k}/k)$ the group of automorphisms of $\bar{k}$ over $k$, $V$ an irreducible scheme projective and smooth over $k$, and

$\bar{V} = V \underset{k}{\times} \bar{k}$ the scheme obtained from $V$ by base extension to $\bar{k}$. For each prime number $\ell$ different from the characteristic of $k$, we put

$$(1) \qquad H^i_\ell(\bar{V}) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} (\varprojlim_n H^i(\bar{V}_{\text{étale}}, \mathbb{Z}/\ell^n\mathbb{Z}))$$

where $\bar{V}_{\text{étale}}$ denotes the étale topology of $\bar{V}$. In the classical case, $\bar{k} = \mathbb{C}$, the comparison theorem of M. Artin allows us to replace "étale" by "classical" in this formula. The inverse limit is then isomorphic to $H^i(\bar{V}_{\text{classical}}, \mathbb{Z}_\ell)$ and consequently we have

$$H^i_\ell(\bar{V}) \approx H^i(\bar{V}_{\text{classical}}, \mathbb{Q}_\ell) \simeq \mathbb{Q}_\ell \otimes_{\mathbb{Q}} H^i(\bar{V}_{\text{classical}}, \mathbb{Z})$$

In the abstract case there is no good cohomology with rational coefficients, and it is the groups $H^i_\ell(\bar{V})$ which play the role which we are accustomed to attribute to "cohomology with coefficients in $\mathbb{Q}_\ell$". I understand that the étale cohomologists have established finite dimensionality, Poincaré duality, Künneth formulas, and a Lefschetz fixed point theorem for the groups $H^i_\ell$. The proper base change theorem shows that the groups $H^i_\ell$ do not change if we replace $\bar{k}$ by a larger algebraically closed field. As Mike Artin said in his talk, the situation is just like in the good old days.

In one respect the situation is even better, because the Galois group $G(\bar{k}/k)$ operates on the groups $H^i_\ell(\bar{V})$. Namely, it operates on the product $\bar{V} = V \times_k \bar{k}$ through the second factor, and hence on the site $\bar{V}_{\text{étale}}$; the point is that the étale topology depends only on $\bar{V}$ and not on the arrow $\bar{V} \longrightarrow \operatorname{Spec} \bar{k}$ which is used to define the classical topology when $\bar{k} = \mathbb{C}$.

There results a homomorphism

$$(2) \qquad G(\bar{k}/k) \longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(H^i_\ell(\bar{V})) \simeq \mathrm{GL}(b_i, \mathbb{Q}_\ell)$$

(where $b_i = \dim_{\mathbb{Q}_\ell} H^i_\ell$ = $i^{\text{th}}$ Betti number). Using the base change theorem one sees that the homomorphism (2) induces a topological isomorphism $G(k'/k) \xrightarrow{\sim} G^i_\ell$ between the group of a certain Galois extension $k'$ over $k$ and a certain closed subgroup $G^i_\ell$ of $\mathrm{GL}(b_i, \mathbb{Q}_\ell)$. Thus the situation is exactly as described by Serre [4] in case $V = A$ is an abelian variety and $i = 1$, when $H^1_\ell(\bar{A})$ can be identified with the dual of Serre's $V_\ell(A)$. The group $G^i_\ell$ is an $\ell$-adic Lie group, whose Lie algebra $\mathfrak{g}^i_\ell$ is unchanged if we replace $k$ by an extension of finite type. These Lie algebras of Serre's raise a host of new problems, even, or perhaps especially, in the classical case.

For example, let $X$ be a complex projective nonsingular variety. Then we can find a field $k \subset \mathbb{C}$ finitely generated over $\mathbb{Q}$, and a scheme $V$ over $k$ such that $\bar{V} = V \times_k \mathbb{C} \simeq X$. The Lie algebras

$$\mathfrak{g}^i_\ell \subset \mathrm{End}_{\mathbb{Q}_\ell}(H^i(X, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$$

which are which are obtained in the manner just discussed are <u>independent of the choice of</u> $k$ <u>and</u> $V$, <u>and depend only on</u> $X/\mathbb{C}$. Almost nothing is known about them, cf. Serre [4]. Is their dimension and type independent of $\ell$? Are they reductive? Serre [5] has shown the answers are affirmative in case $X$ is a complex torus of dimension 1 whose $j$ invariant is either real, or not an algebraic integer. The conjecture about algebraic cycles which I

am going to discuss in a moment has the following consequence in the present situation: Let $\omega \in H^2(X, \mathbb{Q})$ be the cohomology class of a hyperplane section. For $x \in \mathcal{V}_\ell^{2i}$, let $x\,\omega^i = \lambda_i(x)\omega^i$, with $\lambda_i(x) \in \mathbb{Q}_\ell$. Let $\theta \in H^{2i}(X, \mathbb{Q})$. Then (conjecturally) some multiple of $\theta$ is the class of an algebraic cycle of codimension $i$ if and only if $x\theta = \lambda_i(x)\theta$ for all $x \in \mathcal{V}_\ell^{2i}$.

§ 2. Cohomology classes of algebraic cycles. The operation of $G(\bar{k}/k)$ on cohomology makes it imperative to keep track of "twisting" by roots of unity. If $G(\bar{k}/k)$ operates on a vector space $H$ over $\mathbb{Q}_\ell$, we define the twistings of $H$ to be the $G(\bar{k}/k)$ spaces $H(m) = H \otimes_{\mathbb{Q}_\ell} W^{\otimes m}$, for $m \in \mathbb{Z}$, where

$$W = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \left( \varprojlim \{\mu_{\ell^n}\} \right) \tag{3}$$

is the one dimensional $\ell$-adic vector space on which $G(\bar{k}/k)$ operates according to its action on the group $\mu_{\ell^n}$ of $\ell^n$-th roots of unity for all $n$ (for $m < 0$, we put $W^{\otimes m} = \mathrm{Hom}(W^{\otimes |m|}, \mathbb{Q}_\ell)$, so that $H(m)(n) \simeq H(m+n)$ for all $m, n \in \mathbb{Z}$). The canonical isomorphisms

$$H^i(V_{\text{étale}}, \mathbb{Z}/\ell^n\mathbb{Z}) \otimes \mu_{\ell^n}^{\otimes m} \xrightarrow{\sim} H^i(V_{\text{étale}}, \mu_{\ell^n}^{\otimes m})$$

(which are obtained by viewing $\mu_{\ell^n}^{\otimes m}$ as $\mathrm{Hom}(\mathbb{Z}/\ell^n\mathbb{Z}, \mu_{\ell^n}^{\otimes m})$) show that if we replace $\mathbb{Z}/\ell^n\mathbb{Z}$ by $\mu_{\ell^n}^{\otimes m}$ in the definition (1) of $H^i_\ell(\bar{V})$, then we replace $H^i_\ell(\bar{V})$ by its $m$-fold twisting $H^i_\ell(\bar{V})(m)$.

Let $d = \dim V$. As Verdier discussed in his talk, the "orientation sheaf (mod $\ell^n$)" on $\bar{V}$ is $\mu_{\ell^n}^{\otimes d}$, and there is a canonical isomorphism

(4) $$\rho_V : H^{2d}_{\ell}(\bar{V})(d) \xrightarrow{\sim} \mathbb{Q}_{\ell} \ .$$

(For practical purposes, "canonical homomorphism" means $G(\bar{k}/k)$ homomorphism.) The $\ell$-adic Poincaré duality theorem states then that the cup product pairing:

$$H^i_{\ell}(\bar{V})(m) \quad \times \quad H^{2d-i}_{\ell}(\bar{V})(d-m) \longrightarrow H^{2d}(\bar{V})(d) \simeq \mathbb{Q}_{\ell}$$

gives a perfect duality of finite dimensional vector spaces.

Thus, if $X$ is an irreducible subscheme of $\bar{V}$ of codimension $i$, we can attach to $X$ a cohomology class $c(X) \in H^{2i}(\bar{V})(i)$ which is characterized by the fact that

$$\rho_V(\eta \cup c(X)) = \rho_X(\eta|X)$$

for all $\eta \in H^{2(d-i)}(\bar{V})(d-i)$. Extending $c$ by additivity we obtain in this way a homomorphism

(5) $$\mathcal{Z}^i(\bar{V}) \xrightarrow{c} H^{2i}_{\ell}(\bar{V})(i) \ ,$$

where $\mathcal{Z}^i(\bar{V})$ denotes the free abelian group generated by the irreducible subschemes of codimension $i$ on $\bar{V}$. These homomorphisms will carry intersection product into cup product:

$$c(X \cdot Y) = c(X) \cup c(Y)$$

whenever $X \cdot Y$ is defined.

Let $\mathcal{Z}^i_h(\bar{V})$ denote the kernel of the homomorphism $c$ in dimension $i$, (that is, the group of algebraic cycles of codimension $i$ on $\bar{V}$ which are "$\ell$-adically homologically equivalent to zero") and put

$$\mathcal{Q}^i(\bar{V}) = \mathcal{Z}^i(\bar{V})/\mathcal{Z}^i_h(\bar{V}) .$$

One has the following conjectural statements.

(a) $\mathcal{Z}^i_h(\bar{V})$ is independent of $\ell$, or perhaps even

(a') $\mathcal{Z}^i_h(\bar{V})$ consists exactly of the cycles numerically equivalent to zero.

(b) $\mathcal{Q}^i(\bar{V})$ is finitely generated, and the map

$$\mathcal{Q}^i(\bar{V}) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}_\ell \xrightarrow{c\otimes 1} H^{2i}(\bar{V})(i)$$

is injective.

Statements (a) and (b) are true in characteristic zero, because we can then imbed $k$ in $\mathbb{C}$ and factor the map $\alpha$ through the finitely generated $\mathbb{Z}$-module $H^{2i}(\bar{V}_{class}, \mathbb{Z})$, for which

$$H^i_\ell(\bar{V}) \simeq H^i(\bar{V}_{classical}, \mathbb{Z}) \otimes \mathbb{Q}_\ell$$

In the abstract case, nothing is known for codimensions $i > 1$, but for $i = 1$, all three statements (a), (a') and (b) are true. Let $\mathcal{Z}^1_n \supset \mathcal{Z}^1_a \supset \mathcal{Z}^1_\ell$ denote the groups of divisors on $\bar{V}$ which are, respectively, numerically, algebraically, or linearly equivalent to zero. The map $\alpha : \mathcal{Z}^1(\bar{V}) \longrightarrow H^2_\ell(\bar{V})(1)$ is obtained by passage to the limit from the composed maps

$$\mathcal{Z}^1 \longrightarrow \mathcal{Z}^1/\mathcal{Z}^1_\ell \simeq H^1(\bar{V}_{étale}, \mathbb{G}_m) \xrightarrow{\delta_n} H^2(\bar{V}_{étale}, \mu_{\ell^n}) ,$$

where $\delta_n$ is the connecting homomorphism in the cohomology sequence derived from the exact sequence

$$0 \longrightarrow \mu_{\ell^n} \longrightarrow \mathbb{G}_m \xrightarrow{\ell^n} \mathbb{G}_m \longrightarrow 0 \tag{6}$$

(see the talk of Mike Artin). For each $n$ the kernel of $\delta_n$ is $\ell^n H^1(\bar{V}_{ét}, \mathbb{G}_m)$,

and (a') and (b) now follow because $\mathcal{Z}^1_a/\mathcal{Z}^1_\ell$ is divisible, and $\mathcal{Z}^1_n/\mathcal{Z}^1_a$ is the torsion subgroup of the finitely generated group $\mathcal{Z}^1/\mathcal{Z}^1_a$.

From now on, we shall assume (a) and (b) hold in whatever situation is discussed. Each irreducible subscheme $X$ of $\bar{V}$ is "defined" over a finite extension of $k$. Thus $X$ is fixed by an open subgroup $U$ of $G(\bar{k}/k)$, and the same is true of its class $c(X)$. There is a conjectural converse of this statement, namely:

CONJECTURE 1. If $k$ is finitely generated over the prime field then the space $c(\mathcal{Q}^1(\bar{V}))\,\Phi_\ell$ consists of those elements of $H^{2i}_\ell(\bar{V})(i)$ whose stabilizer is open in $G(\bar{k}/k)$, that is, which are annihilated by the corresponding Lie algebra.

Let $\mathcal{Q}^i(V)$ denote the subgroup of $\mathcal{Q}^i(\bar{V})$ generated by the algebraic cycles which are defined over $k$. If an element of $\mathcal{Q}^i(\bar{V})$ is fixed by $G(\bar{k}/k)$, then some non-zero multiple of it is in $\mathcal{Q}^i(V)$. Thus conjecture 1 implies

$$c(\mathcal{Q}^1(V))\Phi_\ell = [H^{2i}_\ell(\bar{V})(i)]^{G(\bar{k}/k)}, \tag{7}$$

for finitely generated $k$. On the other hand, if (7) holds for all (sufficiently large) finite extensions of $k$ then conjecture 1 is true.

Let now $A$ and $B$ be abelian varieties over $k$. If we combine the fundamental isomorphism

$$\mathrm{Hom}_k(A,B) \xrightarrow{\sim} \mathrm{Ker}(\mathcal{Q}^1(A \times \hat{B}) \longrightarrow \mathcal{Q}^1(A) \times \mathcal{Q}^1(\hat{B}))$$

with the Künneth formula

$$H^1_\ell(A) \otimes H^1_\ell(\hat{B}) \xrightarrow{\sim} \mathrm{Ker}(H^1_\ell(A \times \hat{B}) \longrightarrow H^1_\ell(A) \times H^1_\ell(\hat{B}))$$

we conclude from (7) applied to $V = A \times \hat{B}$ with $i = 1$ that

$$\mathrm{Hom}_k(A, B) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} [H^1_\ell(A) \otimes H^1_\ell(\hat{B})(1)]^{G(\bar{k}/k)}$$

is an isomorphism. Reinterpreting the right hand side in terms of points of finite order (via the Kummer sequence (6)) one finds that this last is equivalent to

$$\mathrm{Hom}_k(A, B) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_{G(\bar{k}/k)}(A(\ell^\infty), B(\ell^\infty)), \tag{8}$$

where $A(\ell^\infty)$ denotes the $G(\bar{k}/k)$-module of points on $A$ of order $\ell^\nu$, all $\nu$, with coefficients in $k$. In down to earth terms, if a group homomorphism $\varphi: A(\ell^\infty) \longrightarrow B(\ell^\infty)$ commutes with the operation of the Galois group for a finitely generated $k$, then for every $N$ there should exist a homomorphism of abelian varieties $\psi_N : A \longrightarrow B$ such that $\psi_N$ coincides with $\varphi$ on the points of order $\ell^N$.

Mumford has verified (8) in case $k$ is finite and $A$ and $B$ are of dimension 1, by lifting the Frobenius endomorphism to characteristic 0, a la Deuring, [1].
Results of Serre [5] show that (8) holds in case $k$ is a number field with at least one real prime, and $A = B$ is of dimension 1. Of course, if (8) holds for $A$ and $B$ of dimension 1, then (7) holds with $V = A \times B$.

I can see no direct logical connection between conjecture 1 and Hodge's conjecture [2] that a rational cohomology class of type $(p,p)$ is algebraic, i.e., rational combination of classes of algebraic cycles (in case

of divisors this is a well known theorem of Lefschetz and is even true over $\mathbb{Z}$). However the two conjectures have an air of compatibility. For example, Grothendieck remarks that each of the two conjectures imply that the Künneth components $c_{a,b}$ of an algebraic class $c$ on a product $V' \times V''$ are algebraic, a statement which seems unknown even in case of the diagonal on the product of a surface with itself in the classical case. By the "Künneth decomposition"

$$c = \sum_{a+b=2i} c_{a,b}$$

of a cohomology class $c \in H_\ell^{2i}(\bar{V}' \times \bar{V}'')(i)$ we mean its expression as a sum of classes $c_{a,b} \in H_\ell^{2i}(\bar{V}' \times \bar{V}'')(i)$ such that $c_{a,b}$ is in the image of $[H_\ell^a(\bar{V}') \otimes H_\ell^b(\bar{V}'')](i)$. Conjecture 1 implies that if $c \in c(\mathfrak{A}^i)\mathfrak{Q}_\ell$ then $c_{a,b} \in c(\mathfrak{A}^i)\mathfrak{Q}_\ell$ for all $a$, $b$. Grothendieck conjectures that the same is true with $\mathfrak{Q}$ instead of $\mathfrak{Q}_\ell$, as would follow from Hodge's conjecture in the classical case.

§ 3. Connections with zeta functions (Finite k). Let $\varphi: \bar{V} \longrightarrow \bar{V}$ be a $\bar{k}$-morphism, and let $\varphi_{i,\ell}$ denote the linear transformation of $H_\ell^i(\bar{V})$ induced by $\varphi$. Then the algebraic number $\Lambda(\varphi)$ of fixed points of $\varphi$ is given by the Lefschetz formula

$$\Lambda(\varphi) = \sum_{i=0}^{2d} (-1)^i \mathrm{Trace}(\varphi_{i,\ell}). \tag{9}$$

It is generally conjectured that

(c) The characteristic polynomial $P_{i,\ell}(t) = \det(1 - \varphi_{i,\ell}\, t)$ has rational

integral coefficients and is independent of $\ell$ .

(d) Suppose that there exists an ample $\omega \in \mathcal{A}^1(\bar{V})$ such that $\varphi^*\omega = q\omega$ for some integer $q > 0$ . Then the endomorphisms $\varphi_{i,\ell}$ are semisimple, and if we write

$$\det(1 - \varphi_{i,\ell}t) = P_i(t) = \prod_{j=1}^{b_i} (1 - \alpha_{ij}t) \tag{10}$$

with complex $\alpha_{ij}$ , we have $|\alpha_{i,j}| = q^{i/2}$ for all $j$ . In characteristic zero (c) is an immediate consequence of the existence of integral cohomology, and (d) can be proved by Kählerian methods (cf. Serre [3]). In characteristic $p$ , both conjectures have been proved for curves and abelian varieties by Weil [8]. When $\varphi$ is the Frobenius morphism, conjecture (d) is the famous conjecture of Weil [9] which started this whole business.

From now on we shall assume (c) and (d) hold in whatever situation is discussed. Let $k = \mathbb{F}_q$ be the finite field with $q$ elements. For any scheme $X$ over $\mathbb{F}_q$, the Frobenius morphism $F_X : X \longrightarrow X$ is defined as the identity map on points, together with the map $f \longrightarrow f^q$ in the structure sheaf. This $F_X$ acts like identity on the site $X_{\text{étale}}$, and therefore induces identity on the cohomology groups $H^i(X_{\text{étale}}, \mathbb{Z}/m\mathbb{Z})$. On $\bar{V} = V \times_k \bar{k}$ we have $F_{\bar{V}} = F_V \times F_{\bar{k}} = \varphi \times \sigma$ , say where $\varphi: V \longrightarrow V$ is the usual Frobenious morphism, and where $\sigma$ is the canonical "generator" of $G(\bar{k}/k)$ . Since $\varphi \times \sigma$ acts as identity on cohomology groups $H^i_\ell(\bar{V})$ , we have $\varphi_{i,\ell} = \sigma_{i,\ell}^{-1}$ , where $\varphi_{i,\ell}$ is the linear transformation of $H^i_\ell(\bar{V})$ induced by the $\bar{k}$-morphism $\varphi \times 1$ , and where $\sigma_{i,\ell}$ is the linear

transformation of $H^i_\ell(\bar{V})$ produced by the operation of $\sigma$ as element of $G(\bar{k}/k)$.

The zeta function of the scheme $V$ (see Serre's talk) is given by

$$\zeta(V,s) = \frac{P_1(q^{-s}) \cdots P_{2d-1}(q^{-s})}{P_0(q^{-s})\, P_2(q^{-s}) \cdots P_{2d}(q^{-s})} \qquad (11)$$

where $d = \dim V$; and where $P_i(t)$ is the characteristic polynomial of Frobenius operating on cohomology of dimension $i$, as in (10). Formula (11) results from Lefschetz' formula (9) for $\Lambda(\varphi^\nu)$ and the definition of $\zeta$; see Weil [9]. Since the "reciprocal roots" $\alpha_{ij}$ of $P_i(t)$ have absolute value $q^{\frac{i}{2}}$, the zeros of $\zeta(V,s)$ are on the lines $Rs = \frac{1}{2}, \frac{3}{2}, \ldots, \frac{2d-1}{2}$, and its poles are on the lines $Rs = 0, 1, 2, \ldots d$. The order of the pole at the point $s = i$ is equal to the number of times $q^i$ occurs as a reciprocal root of $P_{2i}(t)$, or what is the same, as an eigenvalue of $\varphi_{2i,\ell}$. By the semisimplicity of $\varphi_{2i,\ell}$, this is the dimension of the space of $x \in H^{2i}_\ell(\bar{V})$ such that $\varphi_{2i,\ell}x = q^i x$, or $x = \sigma_{2i,\ell}q^i x$. Now $\sigma$ operates as $q$ on our twisting space, $W$, because $\sigma$ raises $\ell^n$-th roots of unity to the $q$-th power. Thus for $y \in W^{\otimes i}$ we have $\sigma y = q^i y$ and $\sigma(x \otimes y) = \sigma_{2i,\ell}x \otimes q^i y = \sigma_{2i,\ell}q^i x \otimes y$. It follows that the dimension we are computing is that of the subspace of all $z \in H^{2i}(\bar{V})(i)$ such that $\sigma z = z$, that is, the dimension of $[H^{2i}(\bar{V})(i)]^{G(\bar{k}/k)}$. If (7) is true we have then

(12) $\qquad$ rank $\mathcal{Q}^i(V)$ = order of pole of $\zeta(V,s)$ at $s = i$,

assuming, as always, that (a), (b), (c), and (d) hold. Moreover, the inequality $\geq$ always holds under those assumptions, and equality in (12) for all (sufficiently large) finite extensions of $k$ is equivalent to Conjecture 1.

I have tried to check (12) in case $V = V_{n,r,p}$ is the hypersurface in projective $r$-space defined by the equation

$$X_0^n + X_1^n + \ldots + X_r^n = 0 \tag{13}$$

over a large finite field $k$ of characteristic $p$ not dividing $n$. Weil [9] has computed the zeta function and hence the order of the pole; it is the determination of the rank of $\mathcal{Q}^i(V)$ which is difficult. There is only one non trivial dimension $i$, namely that for which $r = 2i + 1$. I have succeeded in the verification of (12) only in two special cases. (I) if $p^\nu \equiv -1 \pmod{n}$ for some $\nu$, and (II) if $p \equiv 1 \pmod{n}$, and $r = 3$, $i = 1$. In case (I) the order of the pole turns out to be equal to the Betti number $b_{2i}$, so the problem is to prove that the algebraic cohomology classes span $H^{2i}_{\ell}(\bar{V})(i)$.

For this we can replace $n$ by its multiple $q + 1$, where $q = p^\nu$, because $V(q+1, r, p)$ dominates $V(n, r, p)$ as the map $X_j \longrightarrow X_j^{\frac{q+1}{n}}$ shows. This gives us the advantage that our hypersurface

$$X_0^{q+1} + X_1^{q+1} + \ldots + X_r^{q+1} = 0$$

has a large group of automorphisms, namely those induced by the group $U$ of projective transformations

$$X_j \longrightarrow \sum a_{ji} X_i$$

where $(a_{ji})$ is a matrix in $\mathbb{F}_{q^2}$ which is unitary with respect to the conjugation $a \longrightarrow \bar{a} = a^q$. John Thompson and I proved that the representation of $U$ on $H^{2i}_{\ell}(\bar{V})$ is the direct sum of the trivial representation and an irreducible one, and the required result follows easily from this. Incidentally, the non-trivial irreducible representation in question, which is of degree $q\,\frac{q^r+1}{q+1}$, seems to be the irreducible representation of lowest degree $> 1$ of the group of $(r+1) \times (r+1)$ unitary matrices $(a_{ij})$ with $a_{ij} \in \mathbb{F}_{q^2}$, $r$ odd.

In case (II), the order of the pole turns out to be equal to the rank of $\mathcal{Q}^i(\bar{V})$ for the surface $V$ in characteristic zero defined by equation (13). Since the rank of $\mathcal{Q}^i$ can only increase under specialization (look at the intersection matrix), equality (12) must hold. The computation of the rank (Picard number) in characteristic zero is made with the aid of the Lefschetz theorem; it turns out to be possible to count the dimension of the space of rational cohomology classes of type $(1,1)$ by regarding the cohomology as a representation space for the commutative group of automorphisms of the form $X_i \longrightarrow \zeta_i X_i$, where $\zeta_i^n = 1$, $0 \leq i \leq r$. The point is that the spaces $H^{2,0}$, $H^{1,1}$, and $H^{0,2}$ have no common irreducible constituents. If we assume the Hodge conjecture then we can treat case II for arbitrary $r = 2i+1$.

§ 4. Connections with zetas (finitely generated k). Let us turn now to the case k is finitely generated over the prime field, rather than finite. We can then construct a projective and smooth morphism $f : X \longrightarrow Y$ of schemes of finite type over $\mathbb{Z}$, with Y regular and X irreducible, whose general fiber is our given morphism $V \longrightarrow (\mathrm{Spec}\ k)$. (The case which has been studied classically is that in which k is an algebraic number field and Y is an open subset of the spectrum of the ring of integers of k such that V has "non-degenerate reduction" at all points of Y.) For each "closed" point $y \in Y$ we let $V_y$ (rather than the conventional $X_y$) denote the fiber $f^{-1}(y)$, and we let k(y) denote the residue field of y, which is finite with (definition) Ny elements, as Serre mentioned in his talk. Thus the scheme $V_y$ over k(y), and the corresponding "geometric fiber" $\overline{V}_y$ over $\overline{k(y)}$, are as discussed in the preceding section, with $q = Ny$. Expressing the zeta function of the scheme X as a product of the zetas of the closed fibers we have

$$\zeta(X, s) = \prod_{\substack{y \in Y \\ y \text{ closed}}} \zeta(V_y, s) . \tag{14}$$

Expressing the zeta functions of the fibers in the form (11) we have then

$$\zeta(X, s) = \frac{\Phi_0(s)\ \Phi_2(s)\ \ldots\ \Phi_{2d}(s)}{\Phi_1(s)\ \ldots\ \Phi_{2d-1}(s)} , \tag{15}$$

where we have put, for $0 \leq i \leq 2d$,

$$(16) \qquad \Phi_i(s) = \prod_{\substack{y \in Y \\ y \text{ closed}}} \frac{1}{P_{y,i}(N_y^{-s})} \quad .$$

The $P_{y,i}(t)$ are of fixed degree (see below) with reciprocal roots $\alpha_{ij}$ of absolute value $(N_y)^{1/2}$ (recall that we assume conjecture (d) of § 3). Therefore, by theorem 1 of Serre's talk the product (16) converges absolutely for $Re\, s > \dim Y + \frac{i}{2}$. It is conjectured that the $\Phi_i$ can be continued meromorphically in the whole s-plane (cf. Weil [11]). At present the continuability is known only in very special cases (see Shimura's talk). From Poincaré duality, we have $\Phi_{2d-i}(s) = \Phi_i(s - d + i)$.

If we replace $Y$ by a non-empty open subscheme in (16), we divide $\Phi_i(s)$ by a product which converges for $Re\, s > \dim Y + \frac{i}{2} - 1$. It follows that (insofar as $\Phi_i$ is extendible there) the zeros and poles of $\Phi_i$ in the strip

$$\dim Y + \frac{i}{2} - 1 < Re\, s \leq \dim Y + \frac{i}{2}$$

depend only on $V/k$ and not on our choice of $X/Y$. It is therefore natural to try to relate the orders of the zeros and poles of $\Phi_i$ at critical places in that critical strip to other invariants of the variety $V/k$. The original idea in this direction is the following striking

CONJECTURE of Birch and Swinnerton-Dyer: The rank of the group of k-rational points on the Picard variety of $V$ is equal to the order of the zero of $\Phi_1(s)$ at $s = \dim Y$ (and of $\Phi_{2d-1}(s)$ at $s = \dim X - 1$, by duality).

If $k = \mathbb{Q}$, and $V$ is an elliptic curve of the form $y^2 = x^3 - Dx$,

$D \in \mathbb{Z}$, there is overwhelming numerical evidence for the fact that $\Phi_1(1) = 0$ if and only if the curve has a rational point of infinite order (cf. Cassel's talk). In case of finite $k$, the conjecture is trivially true, amounting to $0 = 0$.

I would like now to discuss the following generalization of (12):

CONJECTURE 2: The rank of $\mathcal{C}^i(V)$ is equal to the order of the pole of $\Phi_{2i}(s)$ at the point $s = \dim Y + i$ (and of $\Phi_{2d-2i}(s)$ at $s = \dim X - i$, by duality).

Notice that the position of the pole considered here is on the boundary of the half-plane of convergence of the product, so that conjecture 2 can be given meaning even without supposing analytic continuation. In this respect it is different from the conjecture of B. and S-D., which presupposes analytic continuation a distance of $\frac{1}{2}$ unit to the left of the line of convergence. On the other hand, the two conjectures are intimately related, at least insofar as the case $i = 1$ of conjecture 2 is concerned. This is not surprising, because both of them relate the order of a function at $s = \dim X - i$ to the rank of a group of divisor classes. For example, let $V \longrightarrow W$ be a morphism of varieties of our type over $k$, whose general fiber $V_w/k(w)$ is also of our type. If $k$ is finite, and $W$ and $V_w$ are curves, then it is easy to see, as I mentioned in Stockholm [7], that conjecture 2 for $V/k$ is equivalent to the conjecture of B. and S-D. for $V_w/k(w)$. In the general situation, the two conjectures, for the three varieties $V/k$, $W/k$, and $V_w/k(w)$ are strongly interrelated *.

* See remark at the end of the talk.

Conjecture 2 has been verified in some special cases. If $k$ is a number field and $V$ the surface $X_0^n + X_1^n + X_2^n + X_3^n = 0$, then Weil [10] has computed $\Phi_2(s)$ as a Hecke L-series. Its pole at $s = 1$ turns out to be equal to the Picard number of $\bar{V}$ if $k$ contains the $2n$-th roots of unity. The corresponding statement is true for the hypersurface $\sum_{i=0}^{r} X_i^n = 0$, $r$ odd, if Hodge's conjecture is true for it.

Henry Pohlmann has verified conjecture 2 for $i = 1$ in case $V$ is an abelian variety of C.M. type in the sense of Shimura-Taniyama [13].

It is interesting to consider the case $k$ a number field, $V = E^m$ the product of an elliptic curve $E$ with itself $m$ times over $k$. For each prime $y$ where $E$ has non-degenerate reduction, put

$$\zeta(E_y, s) = \frac{\left(1 - \varepsilon_y N\mathfrak{y}^{\frac{1}{2}-s}\right)\left(1 - \bar{\varepsilon}_y N\mathfrak{y}^{\frac{1}{2}-s}\right)}{\left(1 - N\mathfrak{y}^{-s}\right)\left(1 - N\mathfrak{y}^{1-s}\right)} ,$$

and let

$$\varepsilon_y = e^{i\theta(y)} , \quad 0 \leq \theta(y) \leq \pi$$

Then we have

$$\Phi_i(s) = \prod_{0 \leq \nu \leq \frac{i}{2}} \left(L_{1-2\nu}\left(s - \tfrac{i}{2}\right)\right)^{\binom{m}{\nu}\left(\binom{m}{i-\nu}\right)} , \tag{17}$$

where

$$L_0(s) = \prod_y \frac{1}{1 - N\mathfrak{y}^{-s}} , \text{ and } L_\nu(s) = \prod_y \frac{1}{(1 - \varepsilon_y^\nu N\mathfrak{y}^{-s})(1 - \bar{\varepsilon}_y^\nu N\mathfrak{y}^{-s})} \tag{18}$$

for $\nu > 0$.

In case $E$ has complex multiplication the $L_\nu(s)$ are Hecke L-series, we have rank $\mathcal{A}^i(\bar{V}) = \binom{m}{i}^2$, and conjecture 2 is easily checked for all $i$.

Suppose now that $E$ has no complex multiplication. Then one finds

$$\text{rank } \mathcal{A}^i(V) = \text{rank } \mathcal{A}^i(\tilde{V}) = \binom{m}{i}^2 - \binom{m}{i+1}\binom{m}{i+1} \quad . \tag{19}$$

Let $c_\nu$ be the order of $L_\nu(s)$ at $s = 1$. Assuming conjecture 2, we conclude from (17) and (19) that

$$c_0 = 1, \quad c_2 = -1, \text{ and } c_{2\nu} = 0 \quad \text{for} \quad \nu > 1 .$$

On the other hand, arguing <u>formally</u> from (18) (I have not investigated the analytical subtleties--this is all heuristic) one finds for $0 \leq a < b \leq \pi$ that the density of the set of primes $y$ such that $a \leq \theta(y) \leq b$ is given by $\int_a^b f(t)dt$, where

$$f(t) = \frac{1}{\pi} \sum_{\nu=0}^{\infty} c_\nu \cos \nu t .$$

Assuming $f(t) = f(\pi - t)$ we conclude that $c_\nu = 0$ for $\nu$ odd, and consequently

$$f(t) = \frac{1}{\pi}(1 - \cos 2t) = \frac{2}{\pi}\sin^2 t$$

I understand that M. Sato has found this $\sin^2$ distribution law experimentally with machine computations. Conjecture 2 seems to offer an explanation for it!

I should say partial explanation, because the assumption $f(t) = f(\pi - t)$ had no justification; it amounts to conjecturing, in this special case, that, for odd $i$, the function $\Phi_i(s)$ has no zero and no pole at $s = \dim Y + \frac{i}{2}$, that is, at the real point on its boundary of convergence. It is tempting to make that conjecture in general (after all, in odd dimensions there are no algebraic cycles to create poles). However it is false; over a finite field with $q^2$ elements it is easy to make varieties (supersingular elliptic curves for example) for which $q$ is a reciprocal root of $P_1$. Perhaps the conjecture is true over number fields. I have no idea what to expect in general.

Another question I would like to raise concerns algebraic cycles on abelian varieties. Let $A$ be an abelian variety of dimension $n$ over $\mathbb{C}$.

(*) Is it true that the ring of rational cohomology classes on $A$ of type $(p,p)$, $0 \leq p \leq n$, is generated over $\mathbb{Q}$ by those of type $(1,1)$? This statement implies both the Hodge conjecture for $A$, and also the fact that every algebraic cycle is homologically equivalent to a rational linear combination of intersections of divisors. Mattuck, [12], has proved that (*) holds "in general". It was by verifying (*) in case of $A = E^m$ (power of an elliptic curve) that I was able to compute the ranks of the groups $\mathcal{Q}^1(E^m)$ in the example discussed above. In terms of a period matrix for $A$, the statement (*) translates into a completely down to earth question which could be explained to a bright freshman and which should be settled one way or the other.

The last thing I wish to discuss is the relation between conjectures 1 and 2. We have already seen their equivalence (modulo (a), (b), (c), (d)) in case k is finite. For infinite k, the relation involves Taniyama's idea of L-series attached to $\ell$-adic representations (cf. [6]).

As Mike Artin explained in his talk, it follows from the theorems of specialization and base change in étale cohomology that the cohomology groups $H^i_\ell(\bar{V}_y)$ are independent of y for $y \in Y_\ell$ (here the $Y_\ell$ denotes the locus $\ell \neq 0$ in Y). To make the statement precise, one chooses a "strict localization" $\bar{O}_y \subset k$ of the local ring $O_y$ of y on Y, and uses the residue field of $\bar{O}_y$ as the algebraic closure $\overline{k(y)}$ of k(y). The decomposition subgroup $D_y = \{\sigma \in G(\bar{k}/k \mid \sigma \bar{O}_y = \bar{O}_y\}$ is then mapped homomorphically onto $G(\overline{k(y)}/k(y))$, the kernel being, by definition, the inertia subgroup $I_y$ of y. As usual, everything is determined up to conjugation by y, but actually depends on the choice of $\bar{O}_y$, which plays the role of a path from the general geometric point, spec $\bar{k}$, to the special one, spec $\overline{k(y)}$. This "path" determines an isomorphism

$$H^i_\ell(\bar{V}_y) \simeq H^i_\ell(\bar{V}) \tag{20}$$

which is compatible with the operation of $D_y$. In particular, the inertia group $I_y$ operates trivially on $H^i_\ell(\bar{V})$ for all $y \in Y_\ell$, so that in its action on $H^i_\ell(\bar{V})$, $G(\bar{k}/k)$ operates through its quotient group, $\pi_1(Y_\ell)$, the fundamental group of $Y_\ell$.

For each closed $y \in Y_\ell$, let $\sigma_y$ be the image in $\pi_1(Y_\ell)$ of an inverse image in $D_y$ of the canonical generator $\tilde{\sigma}_y$ of $G(\overline{k(y)}/k(y))$.

(Thus, $\sigma_y$ is determined by $y$ up to conjugation, and in case $k$ is a number field, it is a "Frobenius substitution" in the classical sense.) The compatibility of (20), together with the fact that $\tilde{\sigma}_y^{-1}$ operates on $H_\ell^i(\bar{V})$ as $\varphi_y$ does (see p. 11), shows that the polynomial $P_{y,i}(t)$ in (16) is given by

$$P_{y,i}(t) = \det(1 - t\sigma_{y,i,\ell}^{-1}) \tag{21}$$

where $\sigma_{y,i,\ell}$ denotes the endomorphism of $H_\ell^i(\bar{V})$ induced by the operation of $\sigma_y$. Thus, <u>the function $\Phi_1$ is completely determined by the scheme $Y$, together with the $\ell$-adic representations $H_\ell^1(\bar{V})$ of the fundamental groups $\pi_1(Y_\ell)$</u>. We are therefore led to the following generalization:

Let $Y$ be a regular irreducible scheme of finite type over $\mathbb{Z}$ with function field $k$. Suppose for each prime $\ell \neq$ char $k$ we have a finite dimensional vector space $H_\ell$ over $\mathbb{Q}_\ell$ on which $\pi_1(Y_\ell)$ operates continuously in such a way that the characteristic polynomial

$$P_y(t) = \det(1 - t(\sigma_y^{-1} | H_\ell)) \tag{22}$$

has coefficients in $\mathbb{Z}$, is independent of $\ell$ for $y \in Y_\ell$, and has complex "reciprocal roots" of absolute value $Ny^\rho$, where $\rho$ is a real number independent of $y$. We then say that $H = (H_\ell)$ is a <u>system of representations of weight $\rho$ over $Y$</u>.

Given such a system, we put

(23) $$L(Y,H;s) = \prod_{\substack{y \in Y \\ y \text{ closed}}} \frac{1}{P_y(Ny^{-s})} ,$$

this product being absolutely convergent for $Re\ s > \rho + \dim Y$. Notice the analogy between this definition and Artin's definition of L-functions (cf. Serre's talk, formula (9)). Comparison of (16), (21), (22), and (23) shows that

(24) $$\Phi_i(s) = L(Y, H^i(\bar{V}) ; s) ,$$

is an L-series for the system of representations $(H^i_\ell(\bar{V}))$ of weight $\frac{i}{2}$ over $Y$. Twisting a system of representations by $m$ decreases its weight by $m$, and translates the corresponding L-function $m$ units:

(25) $$L(Y, H(m);s) = L(Y, H, s - m) .$$

Thus

$$\Phi_{2i}(s - i) = L(Y, H^{2i}(\bar{V})(i); s)$$

belongs to the representation system $H^{2i}(\bar{V})(i)$ of weight 0. Conjecture 2 states that the pole of this function at $s = \dim Y$ is of order rank $\mathcal{Q}^i(V)$. Conjecture 1 states that rank $\mathcal{Q}^i(V)$ is equal to the dimension of the subspace of $H^{2i}(\bar{V})(i)$ which is fixed under $\pi_1(Y)$. If we assume the $\pi_1(Y_\ell)$-modules $H^i_\ell(\bar{V})$ are semisimple (as Serre and Grothendieck believe) then the equivalence of conjectures 1 and 2 would follow from

CONJECTURE 3: For some class of representation systems $H = (H_\ell)$ of weight 0 over Y, including at least those of the form $H = (H_\ell^{2i}(\bar{V})(i))$, the order of the pole of $L(Y,H;s)$ at $s = \dim Y$ is equal to the number of times the identity representation occurs in $H_\ell$ (this being independent of $\ell$ ).

Of course, conjecture 3 is true for ordinary Artin L-series (cf. Theorem 6 of Serre's talk), and for Hecke's L-series. I conclude this talk with the hope it is true in far greater generality.

Afterthought 1: On page 1, and hence throughout, it was intended that $\bar{V}$ be irreducible. This was not essential, but merely to fix ideas and simplify statements.

* Afterthought 2: A closer look at the situation V, W, and $V_w$ discussed on page 19 leads to the following consideration. Let X be a regular scheme of finite type over $\mathbf{Z}$ whose zeta function $\zeta(X,s)$ can be meromorphically continued to the point $s = \dim X - 1$. Let $e(X)$ be the order of $\zeta(X,s)$ at that point, and put

$$z(X) = \operatorname{rank} H^0(X, \underline{O}_X^*) - \operatorname{rank} H^1(X, \underline{O}_X^*) - e(X)$$

If one removes from X a closed irreducible subscheme Z of codimension 1, then $z(X)$ does not change. Thus, $z(X)$ is a birational invariant, and

depends only on the function field of $X$. Suppose now $f: X \longrightarrow Y$ with general fiber $V/k$ is as discussed at the beginning of § 4 (so $f$ projective smooth, $Y$ regular, and $\overline{V}$ irreducible.) Then it is easy to see that any two of the following statements imply the third:

(i) the conjecture of Birch and Swinnerton-Dyer for $V/k$,

(ii) the conjecture 2, for $i = 1$, for $V/k$,

(iii) $z(X) = z(Y)$.

Since we have $z(X) = 0$ if $X$ is the spectrum of a finite field, or of the ring of integers in an algebraic number field, and since $z(X)$ is a birational invariant, we can conclude $z(X) = 0$ for all $X$ if (i) and (ii) hold for all $V$. We are thus led to

CONJECTURE 4: If $X$ is a regular scheme of finite type over $\mathbf{Z}$, then the order of $\zeta(X, s)$ at the point $s = \dim X - 1$ is equal to rank $H^0(X, \underline{O}_X^*)$ - rank $H^1(X, \underline{O}_X^*)$.

BIBLIOGRAPHY


[1] Deuring, M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamburg, 14, 1941, p. 197-272.

[2] Hodge, W. V. D., Address at the International Congress of Mathematicians, Cambridge, Mass., 1950.

[3] Serre, J.-P., Analogues Kählériens de certaines conjectures de Weil, Ann. of Math., 1960 or 61.

[4] Serre, J.-P., Sur les groupes de congruence des variétés abéliennes, Izv. Akad. Nauk. SSSR, 28, 1964, p. 3 - 20.

[5] Serre, J.-P., Groupes de Lie $\ell$-adiques attaches aux courbes elliptiques, colloque de Clermont-Ferrand, April, 1964.

[6] Taniyama, Y., $L$-functions of number fields and zeta functions of abelian varieties, J. Math. Soc. Japan, 9 (1957) 330- 366.

[7] Tate, J., Duality theorems in Galois cohomology, Proceedings of the International Congress of Mathematicians, Stockholm, 1962, p. 288-295.

[8] Weil, A., Variétés abéliennes et courbes algébriques, Paris, 1948.

[9] Weil, A., Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc., 55, 1949, p. 497-508.

[10] Weil, A., Jacobi sums as "Grössencharaktere", Trans. A.M.S., 73, 1952, p. 487-495.

[11] Weil, A., Abstract versus classical algebraic geometry, Proceedings of the International Congress of Mathematicians (Volume III) Amsterdam, 1954, p. 550 -558.

[12] Mattuck, A., Cycles on abelian varieties, Proceedings A.M.S., 9, 1958, p. 88-98.

[13] Shimura, G. and Taniyama, Y., Complex multiplication of abelian varieties and its application to number theory, Publ. Math. Soc. Japan, No. 6, 1961.

# ARITHMETIC ON ABELIAN VARIETIES, ESPECIALLY OF DIMENSION 1.

J. W. S. Cassels

An Abelian Variety of dimension 1 defined over a field $k$ is just an elliptic curve together with a point $\underline{o}$ on the curve, all defined over $k$. The law of addition is that $\underline{x} + \underline{y} = \underline{z}$, where $\underline{x}, \underline{y}, \underline{z}$ are points on the curve (not necessarily defined over $k$), if the divisor consisting of $\underline{x}$ and $\underline{y}$, each with multiplicity $+1$, is linearly equivalent on the curve to $\underline{z}$ and $\underline{o}$.

Every elliptic curve $D$ defined over $k$ determines an Abelian Variety of dimension 1 $(C, \underline{o})$ defined over $k$ which is unique (up to birational equivalence over $k$), namely its Jacobian. The usual Jacobian map of divisors of degree 0 on $D$ into points of $C$ gives $D$ a structure $\mu$ of (principal) homogeneous space over $(C, \underline{o})$ defined over $k$. Namely we define $\underline{X} + \underline{y} = \underline{Z}$, where $\underline{X}, \underline{Z}$ are on $D$ and $\underline{y}$ is on $C$ to mean that the divisor consisting of $\underline{X}$ with multiplicity $+1$ and $\underline{Z}$ with multiplicity $-1$ is mapped onto $\underline{y}$ by the Jacobian map. It is readily verified that this does give a homogeneous space defined over $k$.

Although $D$ determines its Jacobian $(C, \underline{o})$ uniquely, the Jacobian map, and so the structure $\mu$ of homogeneous space, is not unique. Clearly given such a structure we can define another by making the sum of $\underline{X}$ and $\underline{y}$ to be $\underline{X} + (-\underline{y})$. Except in the special case when $C$ has complex multiplication by roots of unity defined over $k$ it may be shown that there are in fact just the two structures of homogeneous space on $D$.

As we are interested only in things up to birational equivalence defined over $k$, we say that two homogeneous spaces $(D,\mu)$ and $(D',\mu')$ are in the same class if there is a birational equivalence over $k$ which takes $D$ into $D'$ and $\mu$ into $\mu'$ (in an obvious sense). In characteristic 0 the classes of homogeneous spaces (for given $k$ and Jacobian $(C,\underline{o})$) can be put into 1-1 correspondence with the elements of a cohomology group $H^1(\Gamma,\overline{\mathcal{O}_f})$, where $\Gamma$ is the Galois group of the algebraic closure $\overline{k}$ of $k$ over $k$ and $\overline{\mathcal{O}_f}$ is the group of points on $(C,\underline{o})$ defined over $\overline{k}$. The right cohomology group to take here is not the one given by all cocycles but only by the cocycles which are defined over a finite extension of $k$, i.e.,

$$H^1(\Gamma,\overline{\mathcal{O}_f}) = \varinjlim_K H^1(\Gamma_{k/K},\mathcal{O}_{fK}),$$

where $K$ runs through all finite normal extensions of $k$. If $(D,\mu)$ is any homogeneous space the corresponding element of $H^1(\Gamma,\overline{\mathcal{O}_f})$ is given by the cocycle $\sigma\mathfrak{A} - \mathfrak{A} = \mathfrak{A}_\sigma \in \overline{\mathcal{O}_f}$ $(\sigma \in \Gamma)$ where $\mathfrak{A}$ is any point on $D$ defined over $\overline{k}$ and the subtraction is that given by the structure $\mu$ of homogeneous space. The group law on $\overline{\mathcal{O}_f}$ gives a group law on $H^1(\Gamma,\overline{\mathcal{O}_f})$ and so a group law on the set $WC = WC(C,k)$ of classes of homogeneous spaces. By construction $WC$ is a torsion group. This is just the group law defined by Weil for classes of homogeneous spaces without the benefit of homological algebra.

Now let $K$ be <u>any</u> overfield of $k$. Anything which is defined over $k$ is also defined over $K$ and so there is a natural map

$$WC(C,k) \longrightarrow WC(C,K)$$

which is easily seen to be a group homomorphism. When $k$ is an algebraic

number field and $K = k_v$ is the completion of $k$ with respect to a valuation $v$ we call this map the localization map at $v$ and denote it by $j_v$. The intersection of the kernels of all the localization maps $j_v$ is the Tate-Šafarevič group $Ш = Ш(C,k)$, which plays an important and still mysterious role in the arithmetical theory.

I devoted the greater part of my Stockholm Oration to $Ш$ and so propose only to remind you of a few salient points before I go on to the main topic of this talk. Since it is a subgroup of $WC$, the group $Ш$ is a torsion group. Many cases are now known where $Ш$ consists of more than one element. However, it is easy to see the $Ш/mШ$ is finite for each positive integer $m$. There is a lot of numerical evidence, but no proof, that $Ш$ does not contain any infinitely divisible elements except 0 (and so that the primary components of $Ш$ are all finite groups) and there is indirect evidence (some of which will be presented below) that $Ш$ itself is finite. Finally, there is a skew-symmetric bilinear form defined on $Ш$ with values in $Q/Z$ whose kernel consists precisely of the infinitely divisible elements: so if there are no infinitely divisible elements, the order of each primary component of $Ш$ is a square. The order of $Ш$, if finite, is also a square.

In my Stockholm Oration I reported rather briefly on some numerical work of Birch and Swinnerton-Dyer and on the conjectures they had made on the basis of it. In the meantime the position has become a little clearer, the conjectures have been made more precise and the evidence more compelli the conjectures seem, however, to be as far away as ever. In describing Proofs of this work I shall be guided by the logical connections that have since been

nated rather than by a strictly historical order.

The success of the theory of adeles and of Tamagawa measure in the theory of linear algebraic groups suggests that these concepts be applied to algebraic groups in general, and, in particular, to Abelian varieties. As before, I confine attention to dimension 1. Let $(C, \underline{o})$ be an Abelian variety defined over an algebraic numberfield $k$. For each valuation $v$ of $k$ we denote by $\mathcal{O}_v$ the group of points defined over $k_v$, endowed with the $v$-adic topology. Then $\mathcal{O}_v$ is compact because $C$ is complete. It is natural to define an <u>adele</u> to be just an element of the compact group $\prod_v \mathcal{O}_v$ (with the product topology). There is a natural injection

$$\mathcal{O} \longrightarrow \prod_v \mathcal{O}_v$$

of the group $\mathcal{O}$ of points defined over $k$ into the adele group: the points of the image are the <u>principal adeles</u>. The subgroup of principal adeles is neither discrete nor closed, in general, which is a contrast with the linear algebraic group case. Indeed it is so only if $\mathcal{O}$ is finite.

Let $\omega$ be a differential of the first kind on $C$ defined over $k$, e.g. $\omega = y^{-1}dx$ if $C$ is given by an equation

$$y^2 = x^3 - Ax - B \qquad (A, B \in k). \tag{1}$$

As in the linear group case $\omega$ gives a normalization of the Haar measure on $\mathcal{O}_v$ is a way to be described. Suppose for simplicity that $C$ is given by (1) and that $\omega = y^{-1}dx$. Then the measure $m_v(E)$ of a subset $E$ of $\mathcal{O}_v$ is just the integral

$$\int_{(x,y) \in E} \frac{1}{|y|_v} \, d_v^+ x$$

where $d_v^+$ is the Haar measure on the <u>additive</u> group $k_v$, appropriately

normalized. The normalization is

$$\text{(i)} \qquad \int_{\mathcal{O}_v} d_v^+ x = 1$$

if $v$ is non-archimedian, where $\mathcal{O}_v$ is the set of $v$-adic units.

(ii) $d_v^+$ is the ordinary Lebesgue measure if $k_v = \underline{\underline{R}}$ and twice the ordinary 2-dimensional Lebesgue measure if $k_v = \underline{\underline{C}}$

It is pretty clear that the measure $m_v$ so defined is invariant under the operation of the group $\mathfrak{O}_{\mathfrak{f}_v}$. We shall be primarily concerned with the measure of the whole group. If $C$ is taken in the form (1) and $v$ is a non-archimedean valuation such that (1) taken modulo the prime ideal belonging to $v$ is an elliptic curve over the residue class field, then we have

$$m_v(\mathfrak{O}_{\mathfrak{f}_v}) = \frac{N_v}{\mathfrak{N}(v)} \tag{2}$$

with the above choice of $\omega$, where $N_v$ is the number of points on the reduced curve and $\mathfrak{N}(v)$ is the number of elements of the residue class field. For the remaining finitely many non-archimedean valuations $m_v(\mathfrak{O}_{\mathfrak{f}_v})$ is a rational number which can, in any individual case, be found after a trivial, if sometimes tedious, computation; and $v$ for archimedean $m_v(\mathfrak{O}_{\mathfrak{f}_v})$ is readily expressed in terms of the periods of $\omega$ (in the classical sense: we are now dealing with $\underline{\underline{R}}$ or $\underline{\underline{C}}$).

The above definition of $m_v$ is not intrinsic, since it depends on the choice of the differential $\omega$ of the first kind. If $\omega'$ is another such differential, then $\omega' = \lambda\omega$ for some $\lambda \in k$ and so

$$m_v'(\ ) = |\lambda^{-1}|_v\, m_v(\ ),$$

where $m_v'$ is defined in terms of $\omega'$ as $m_v$ is in terms of $\omega$. Hence

$$\tau^{-1} = [\tau(C,k)]^{-1} = \prod_{\text{all } v} m_v(0_v), \qquad (3)$$

if the product converges, is independent of the choice of $\omega$ and so depends only on $C$ and $k$. It is the measure of the entire adele group in the product-measure of the $m_v$ (the Tamagawa measure) (if it exists).

Birch and Swinnerton-Dyer conjecture that it is always possible to gove a sense to the right hand side of (3) as a positive real number or $+\infty$, possibly by interpreting the product in some heuristic way (see below). They then conjecture, further, that

$$\tau = \frac{\#(Ш)}{[\#(0_f)]^2}, \qquad (4)$$

where $\#(S)$ denotes the number of elements of a set $S$. This conjecture presupposes the conjecture that $\#(Ш)$ is finite, and the right hand side of (4) is interpreted as $0$ if $\#(0_f)$ is infinite.

Birch and Swinnerton-Dyer started off by considering the behavior of the partial products of the product

$$\prod_{v \text{ "good"}} \frac{N_v}{\gamma_k(v)} \qquad (5)$$

for certain special curves $C$, the ground field being the rationals. To them, as experienced computers, the results were sufficiently promising to call for further investigation. They then noted that for a "good" valuation $v$ (i.e., a non-archimedean valuation with a good reduction) the local zeta-function is given by:

$$\zeta_v(s) = \frac{f_v(s)}{[1-(\gamma_k(v))^{s}][1-(\gamma_k(v))^{1-s}]}$$

where

$$f_v(s) = 1 + (N_v - \gamma_k(v) - 1)(\gamma_k(v))^{-s} + (\gamma_k(v))^{1-2s},$$

$$f_v(1) = n_v/\gamma_k(v). \qquad (6)$$

A conjecture of Hasse (which is a special case of a later conjecture of Weil) is that

$$\prod_v \zeta_v(s),$$

which is convergent if the real part of $s$ is large enough, is analytically continuable over the plane as a meromorphic function. This conjecture implies, in particular, that

$$L(s) = \prod_{v \text{ good}} [f_v(s)]^{-1} \tag{7}$$

defines a meromorphic function on the whole plane and, after (3), (6), it is natural to put

$$\tau = L(1) \cdot \prod_{v \text{ "bad"}} [m_v(\mathfrak{O}_v)]^{-1}$$

($v$ is "bad" if it isn't good). In the particular case when $C$ has complex multiplication it was shown by Deuring that Hasse's conjecture is true, and that in fact $L(s)$ is a Hecke $L$-function with Grössencharakter. (This is a special case of later results of Shimura and Taniyama.) Birch and Swinnerton-Dyer then mounted an all-out attack on the special case $k = \mathbb{Q}$ and $C$ given by:

$$y^2 = x^3 - Dx, \qquad D \in \mathbb{Z} \tag{8}$$

(so complex multiplication by $i$). They managed to find an expression for $L(1)$ as a finite sum of the type

$$\sum_{\vartheta} \chi(\vartheta)\, \ell(\vartheta) \tag{9}$$

where $\ell$ is a certain function defined on the curve $y^2 = 4x^3 - 4x$, $\vartheta$ runs through the group $\Delta$ of all $D$-division points on this curve and $\chi$ is a character on $\Delta$. Application of Galois theory to this formula shows that $\tau$ is rational and permits an estimate of the denominator. The sum is,

however, far too loathesome to be evaluated by hand. Birch and Swinnerton-Dyer used the machine to evaluate $T$ for a large number of values of $D$ and also to find $\mathcal{O}_J$. (As I explained in my Stockholm Oration there is no sure-fire algorithm for finding $\mathcal{O}_J$ but experience shows that it can usually be done.) They found the following experimental facts, both in accordance with the conjecture (4):

(i) $T = 0$ if and only if $\#(\mathcal{O}_J) = \infty$

(ii) $T$ is always a nonnegative square.

This tallies with (4) because, as I explained, $\#(\ )$ must be a perfect square if it is finite. Further, the actual values of $T$ obtained agree with what is known about $Ш$. (This is precious little except for the 2- and 3-components. Some of the values of $T$ suggest that $Ш$ must contain elements of order 5 or 7 but no one has yet found a feasible way of actually exhibiting them because the numerical work would be so difficult.)

Quite recently I have found other evidence for (4) by considering a pair $C_1, C_2$ of isogenous curves. F. K. Schmidt showed that two elliptic curves over a finite field have the same number of points defined over the field. In an obvious notation (2) then implies that

$$m_v(\mathcal{O}_{J_{1v}}) = \frac{N_{1v}}{\mathcal{N}(v)} = \frac{N_{2v}}{\mathcal{N}(v)} = m_v(\mathcal{O}_{J_{2v}})$$

for all except a finite number of $v$ and so that

$$\prod_{\text{all } v} \frac{m_v(\mathcal{O}_{J_{2v}})}{m_v(\mathcal{O}_{J_{1v}})} = T(C_1/C_2) \quad \text{(say)} \tag{10}$$

is well defined. It can be shown that

$$T(C_1/C_2) = \frac{\#\{\mathcal{O}_{J_2}/\nu_1\mathcal{O}_{J_1}\}\#\{(\mathcal{O}_{J_2})_{\nu_2}\}\#\{(Ш_1)_{\nu_1}\}}{\#\{\mathcal{O}_{J_1}/\nu_2\mathcal{O}_{J_2}\}\#\{(\mathcal{O}_{J_1})_{\nu_1}\}\#\{(Ш_2)_{\nu_2}\}} \tag{11}$$

where $v_1 : C_1 \to C_2$ $\quad v_2 : C_2 \to C_1$

is a conjugate pair of isogenies and where, say $(Ш_1)_{v_1}$ denotes the kernel of the map $Ш_1 \to Ш_2$ induced by $v_1$. This formula is proved without any hypothesis about the finiteness of $\mathcal{O}_J$ and $Ш$: all the terms on the right hand side are natural numbers. But now (3) and (10) imply that we should have

$$T(C_1/C_2) = \tau(C_1)/\tau(C_2)$$

and in fact (11) is just what one does get on taking the ratios of the right hand sides of (4) with $C = C_1, C_2$ and noting that

$$\#[(Ш_1)_{v_1}] = \#[Ш_1/v_2 Ш_2]$$

by the functorial properties of the bilinear form on $Ш$ which I mentioned at the beginning.

It is worth noting, too, that the factor $\#(Ш)$ in (4) is quite analogous to a factor which occurs in Ono's formula for the Tamagawa Numbers of tori. On the other hand the factor $\#(\mathcal{O}_J)^2$ seems to me rather surprising as the results for linear groups are for the Tamagawa measure of the quotient group (adeles / modulo principal adeles)and rather suggest that one should get only $\#(\mathcal{O}_J)$. It would be interesting to get a conjecture for <u>all</u> algebraic groups.

There is a second Birch - Swinnerton - Dyer conjecture, this time about the rank, i.e., the number of generators of infinite order, of the finitely generated group $\mathcal{O}_J$. (The finite generation of $\mathcal{O}_J$ is, of course, the Mordell - Weil theorem.) Their preceding conjecture implies that $L(s)$ given by (7) has a zero at $s = 1$ if and only if the rank $g$ is not zero. They conjecture further, that the order of the zero is just $g$. This

conjecture has been taken up by Tate, and it is now a special case of a really grandiose conjecture, but I am not competent to discuss these higher flights of fancy. One way of checking the conjecture would be to evaluate the successive derivatives of $L(s)$ at $s = 1$ and compare this with what is known about $\mathfrak{Ш}$, but no one has yet had the fortitude to attempt this. However recently, Birch, following up a suggestion of Shimura, has noted that at least in the special case (8) one can determine the <u>parity</u> of the order of the zero of $L(s)$ at $s = 1$ from the functional equation of the $L$-function (our notation is unorthodox, our $s = 1$ corresponds to $s = 1/2$ on the critical line in a properly chosen notation). On the other hand, a simple argument using (11) gives the <u>parity</u> of $g$ under the conjecture that $\mathfrak{Ш}_1$, $\mathfrak{Ш}_2$ are finite. And Birch shows by a rather tedious elementary transformation that the two parities are the same.

This is only a report on work in progress and has the untidyness [illegible] of such a report. It seems to me that the evidence for the Birch - Swinnerton-Dyer conjectures taken all in all is overwhelming but it seems likely that essentially new ideas will be needed to obtain proofs.

# SOME REMARKS CONCERNING THE ZETA FUNCTION OF AN ALGEBRAIC VARIETY OVER A FINITE FIELD.

B. Dwork

Let us begin by considering an elementary application of p-adic analysis to the theory of the zeta function. How does one know that the inverse roots and poles are algebraic integers. The theorem is due to Fatou (Acta Mathematica 1906 p. 364). Suppose $\prod (1 - \alpha_i t) / \prod (1 - \beta_j t) = 1 + c_1 t + c_2 t^2 + \dots$ where the $\alpha_i$ and $\beta_j$ are finite in number and are algebraic numbers while $c_1, c_2, \dots$ are rational integers. If $p$ is any prime consider the right hand side when the p-adic value of $t$ is strictly less than $1$. Clearly the series converges and the limit has p-adic value $1$. Hence neither $\alpha_i^{-1}$ nor $\beta_j^{-1}$ can have p-adic value strictly less than $1$ and thus each $\alpha_i$ and $\beta_j$ must be an algebraic integer.

A common phenomenon in p-adic analysis is that if a function $g(x)$ is analytic in some region then the function $g(x)/g(x^p)$ has an analytic continuation to a somewhat larger region. Some examples of this will be given

(a) Let $m$ be an integer prime to $p$ and consider $g(x) = x^{1/m}$ analytic for $x$ close to $1$ ($g(1) = 1$), then $g(x)/g(x^p) = x^{(1-p)/m}$ which is rational if $m$ divides $p - 1$ and while $g(x)$ converges only for $|x - 1| < 1$, $g(x)/g(x^p)$ has a continuation to all $x \neq 0$. Furthermore when $x = x^p$ the ratio gives the $m^{th}$ power residue in the field of $p$ elements.

(b) A less trivial example is given by $g(x) = (1 + x)^{1/m}$ where $m$ is as above. In this case $g(x)/g(x^p)$ has an analytic continuation (if $m$ divides $p - 1$) to a disc properly containing the unit disk $|x| \leq 1$ from which we must remove the disk $|x - 1| < 1$. Here again the value of the extension of the ratio at $x = x^p$, $x \neq 1$ is precisely the $m^{th}$ power residue of $1 + x$.

(c) One of the original observations involved the hypergeometric series $F(\frac{1}{2}, \frac{1}{2}, 1, \lambda) = \sum_{j=0}^{\infty} \binom{-\frac{1}{2}}{j}^2 \lambda^j$ which converges for $|\lambda| < 1$ ($p \neq 2$) and here the ratio $F(\frac{1}{2}, \frac{1}{2}, 1, \lambda)/F(\frac{1}{2}, \frac{1}{2}, 1, \lambda^q)$ has an analytic continuation to the "closed" unit disk provided you delete the disks defined by

$$\left| \sum_{j=0}^{(p-1)/2} \binom{-\frac{1}{2}}{j}^2 \lambda^j \right| < 1 .$$

(No doubt the region of analyticity is somewhat larger.) According to an unpublished theorem of Tate, when $\lambda = \lambda^q$, the value assumed by the ratio is one of the non-trivial roots of the zeta function of the reduction of the elliptic curve $y^2 = x(x-1)(x - \lambda)$ provided the Hasse invariant is not zero.

(d) The most important example is given by the case $g(x) = \exp(\pi x)$ where $\pi^{p-1} = -p$. Here $g(x)/g(x^p) = \exp(\pi(x - x^p))$ converges for ord $x > -(p-1)/p$ and the ratio may be viewed as the composition $g(x - x^p)$ if $|x| < 1$ but not if $|x| \geq 1$. In particular $(g(x)/g(x^p))^p = \exp(p\pi(x - x^p)) = g(p(x - x^p))$ may be viewed as the

composite function for $|x| = 1$ and hence when $x = x^p$, the ratio $g(x)/g(x^p)$ takes on the $p^{th}$ roots of unity as values. In this way an analytic representation of the additive characters of finite fields is obtained. Aside from the estimate for domain of convergence the above remains valid if $\pi$ is replaced by $\pi'$ where $|\pi - \pi'| < 1$.

We now explain briefly how example (c) can be generalized for all non-singular hypersurfaces.

Let $\Omega$ be the completion of the algebraic closure of the p-adic rationals. Let $f(x)$ be a homogeneous polynomial of degree $d$ in $x = (x_1, \ldots, x_{n+1})$ with coefficients in the ring of integers of $\Omega$ and suppose that the reduced hypersurface defined by $f \equiv 0 \bmod p$ is nonsingular and in general position (i.e., the intersection with each linear subvariety $X_{i_1} = x_{i_2} = \ldots = x_{i_r} = 0$ is again non-singular. Let $x_0$ be another indeterminate and let $\mathcal{L}^*$ be the subspace of $\Omega[[\frac{1}{x_0}, \ldots, \frac{1}{x_{n+1}}]]$ "spanned" by elements of type $1/x^w$ where $dw_0 = w_1 + \ldots + w_{n+1}$. Let $K$ be the space of elements, $\xi^*$, in $\mathcal{L}^*$ such that

$$E_i\xi^* + \pi\gamma_- \; x_0 f_i \xi^* = 0, \quad i = 1, 2, \ldots, n+1$$

where $E_i = x_i \frac{\partial}{\partial x_i}$, $f_i = E_i f$ and $\gamma_-$ simply means discard all terms of $x_0 f_i \xi^*$ which obviously do not lie in $\mathcal{L}^*$. The dimension of $K$ is $d^n$ (for this it is enough if $f$ is nonsingular in characteristic zero and in general positico in that sense) and each element of $K$ satisfies

certain growth conditions (here we use the hypothesis in characteristic p). The zeta function of the reduced hypersurface is determined by the non-singular endomorphism

$$\alpha^* = \gamma_- \circ \frac{\exp \pi x_0^q f(x^q)}{\exp \pi x_0 f(x)} \circ \bar{\Phi}$$

of $K$, where $\bar{\Phi}$ maps $1/x^w$ into $1/x^{qw}$, provided the reduced polynomial $\bar{f}$ has coefficients in the field of $q$ elements. The theory may appear to depend on the lifting $f$ of $\bar{f}$ but in fact if $F$ is another lifting of $\bar{f}$ to $\Omega[x]$, then there exists a natural mapping $\xi^* \longrightarrow \gamma_- \xi^* \exp(\pi x_0(f - F))$ of $K$ onto $K'$ and from this the essential uniqueness of the construction follows. This mapping can be checked directly but to obtain insight we suggest the heuristic argument that $D_i^*$ is "essentially" $\exp(-\pi x_0 f(x)) \circ E_i \circ \exp(\pi x_0 f(x))$ and that $\alpha^*$ is "essentially" $\exp(-\pi x_0 f(x)) \circ \bar{\Phi} \circ \exp(\pi x_0 f(x))$.

A more systematic examination of this mapping of $K$ onto $K'$ leads to the proposed extension of example (c) above. We first consider a family, $f(x, T)$, of hypersurfaces of degree $d$ in $x_1, \ldots, x_{n+1}$ parametrized by a new indeterminate, $T$. As before we construct $K_T$ but here the elements lie in $\Omega(T)[[\frac{1}{x_0}, \frac{1}{x_1}, \ldots, \frac{1}{x_{n+1}}]]$. Let $R(T)$ be the resultant of $E_1 f(x, T), \ldots, E_{n+1} f(x, T)$, viewed as polynomials in $x_1, \ldots, x_{n+1}$. We construct a basis of $K_T$ of the form

$$\xi_{u,T}^* = \frac{1}{g(T)} \sum \frac{1}{x^w} \frac{G_{u,w}(T)}{\pi^{w_0} R(T)^{w_0}}$$

indexed by u running through a suitable indexing set. Here $g(\Gamma)$ is a fixed polynomial and $G_{u,w}(\Gamma) \in \underline{O}[\Gamma]$ for all u, w and aside from the zeros of $g(\Gamma)$ (which shall be ignored in the future) the basis can be specialized, given series with good growth conditions provided $|R(\Gamma)| = 1$, $|\Gamma| \leq 1$.

For $\Gamma$ close to zero, (we now redefine $K_\Gamma$ as imbedded in $\mathcal{L}^*$) we have a natural mapping, $\gamma_- \circ \exp \pi x_0 (f(x,\Gamma) - f(x,0))$ of $K_0$ onto $K_\Gamma$ (we suppose $R(0) \not\equiv 0$) ; relative to our bases this mapping has matrix $C_\Gamma$ which satisfies a system of ordinary linear differential equations with rational coefficients and we obtain the commutative diagram

$$\begin{array}{ccc} K_0 & \longrightarrow & K \\ \Big\downarrow{\scriptstyle a_0^*} & & \Big\downarrow{\scriptstyle \Gamma^q} \\ K_0 & \longrightarrow & K_\Gamma \end{array} \qquad a_\Gamma^*$$

where $a_\Gamma^* = \gamma_- \circ \dfrac{\exp(\pi x_0^q f(x^q, \Gamma^q))}{\exp(\pi x_0 f(x,\Gamma))}$

Writing this in matrix form

$$a_\Gamma^* = C_{\Gamma^q}^{-1} a_0^* C_\Gamma$$

and $a_\Gamma^*$ can be shown to be holomorphic in a disk $|\Gamma| < b$ where $b > 1$ provided the region $|R(\Gamma)| < 1$ is deleted as well as the isolated zeros of $g(\Gamma)$ in the formula for the basis. If we let $K_\Gamma^s$ denote the elements, $\xi^*$, of $K_\Gamma$ which have the property that no single monomial $\dfrac{1}{x^w}$ occurring in $\xi^*$ involves all the variables and if we let $\overline{K}_\Gamma = K_\Gamma / K_\Gamma^s$

then the above theory remains valid and the functional equation of the zeta function of the reduced hypersurface $f(x,\Gamma) = 0$ where $\Gamma$ is specialized to say $\Gamma^q = \Gamma$ has been proved (On the zeta function of a Hypersurfaces II, Annals of Math. 1964) by proving that $C_\Gamma^t J C_\Gamma$ is a rational matrix function of $\Gamma$, $J$ being a suitable constant nonsingular matrix.

For elliptic curves, $C_\Gamma$ is formally the period matrix for integrals of the second kind while for the case of a variety of dimension $0$, say $f(x_1,x_2,\Gamma) = x_1^d + \Gamma h(x_1,x_2) - 1$, where $h$ is homogeneous of deg $d$, the meaning of $C_\Gamma$ (as transformation of $\bar{K}_0$ onto $\bar{K}_\Gamma$) can be explained as follows. Classically, let $y_1,\ldots,y_d$ be the zeros of the polynomial

$$f(y,1,\Gamma) = 0$$

viewed as holomorphic functions of $\Gamma$ for $\Gamma$ close to zero such that $y_j \longrightarrow w^j$ as $\Gamma \longrightarrow 0$, $w$ being a primitive $d^{th}$ root of unity. Let $P_\Gamma$ be the Vandemonde matrix

$$\left(\frac{y_i^j}{f'(y_i,1,\Gamma)}\right) \qquad \begin{matrix} j = 1,2,\ldots,d-1 \\ i = 1,2,\ldots,d \end{matrix}$$

then $P_0 C_\Gamma = P_\Gamma$, where $f'(y,1,\Gamma) = \frac{\partial}{\partial y} f(y,1,\Gamma)$. (multiplication of $d \times (d-1)$ matrix by $(d-1) \times (d-1)$ matrix).

The interpretation of the matrix of $\alpha_\Gamma^*$ relative to our basis in the zero dimensional case should be of some interest. If $\Gamma$ is specialized so that $\Gamma^q = \Gamma$ and $\bar{f}$ has coefficients in the field of $q$ elements then $\alpha_\Gamma^*$ should represent the Frobenius operating on the splitting

field of $\bar{f}(y,1,\Gamma)$ over the field of $q$ elements. If $f$ has integral coefficients say in $\mathbf{Z}$, then the construction of the basis of $K_\Gamma$ is independent of $p$ and it seems possible that if $\Gamma_0$ is a fixed element of $\mathbf{Z}$ and if for each prime $p$ (excluding primes which divide $R(\Gamma_0)$, in this case the discriminant), we specialize $\Gamma$ so that $\Gamma \equiv \Gamma_0 \bmod p$, $\Gamma^q = \Gamma$, then the matrices $\alpha_p$ obtained in this way represent in a uniform manner the Frobenius automorphisms associated with the splitting field of $f(y,1,\Gamma_0)$. (It need hardly be mentioned that the theory can be formulated so as to avoid the condition $\Gamma^p = \Gamma$). The analytic properties of $\alpha^*_\Gamma$ may be of interest in the study of L-series.

An annoying feature of the theory is the requirement that $f(x)$ be nonsingular and in general position. Thus the theory cannot be applied directly to elliptic curves in Legendre normal forms and more seriously to the case of genus 2. To overcome this difficulty as well as for intrinsic interest we propose to extend the theory to the singular case. The problems are homological. Associated with $D_1^*, \ldots, D_{n+1}^*$ we can form the sequence

$$0 \longrightarrow \mathcal{L}^* \longrightarrow \mathcal{L}^{*\,(n+1)}_1 \longrightarrow \mathcal{L}^{*\,(n+1)}_1 \longrightarrow \cdots$$

and form homology spaces $H^0(\mathcal{L}^*) = K$, $H^{(1)}(\mathcal{L}^*)$, $H^{(2)}(\mathcal{L}^*)$, etc. It is also of interest to extend the notion of $K$ by defining

$$K^{(r)} = \{\xi^* \in \mathcal{L}^* \mid D_1^{*a_1} \cdots D_{n+1}^{a_{n+1}} \xi^* \text{ whenever } a_1 + \cdots + a_{n+1} \geq r\}$$

and letting $K^{(\infty)} = \bigcup K^{(r)}$. In the nonsingular case (general position)

$H^{(j)}(\mathcal{L}^*) = H^{(j)}(K^{(\infty)}) = 0$ for $j \geq 1$ while in the general case we can show that

$$\dim H^{(j)}(\mathcal{L}^*) < \infty$$

and is uniformly bounded independently of dimension and the same holds for $H^{(1)}(K^{(\infty)}$ and of course for $H^{(0)}(K^{(\infty)})$. Furthermore we can show that if $f$ is defined over $\mathbb{Z}$ (more generally over ring of integers of algebraic number field) then the elements of $K^{(\infty)}$ have good growth conditions for almost all $p$. This means that for almost all $p$, $a^*$ operates on $K^{(\infty)}$ and in fact determines the zeta function of the reduced variety. This is of interest only if $f$ is singular (or not in general position) in characteristic zero. We conjecture that in some formal sense the zeta function of the reduction of $f$ is independent of $p$ for almost all $p$ if $f$ is defined over $\mathbb{Z}$ and it is clear that this is certainly the case if $\dim H^{(j)}(K^{(\infty)})$ is finite for all $j$.

In any case the dimension of $K^{(n+1)}$ is finite and the zeta function is determined by the action of $a^*$ on the elements of $K^{(n+1)}$ with good growth conditions.

In conclusion I would like to mention extensions to complete intersections and other varieties by Ireland (Doctoral Thesis, Johns Hopkins 1964). Of particular value in such extensions is a general unmixedness theorem of W. L. Chow. This theorem is of value in establishing growth conditions for $K$ in the extended situations treated by Ireland. In these extensions the theory has reached a point equivalent to Theorem 4.2 of Hypersurfaces I (Pub. No. 12 IHES), and it seems likely that the verification of the functional equation may be achieved by an inductive argument.

# THE ZETA-FUNCTION OF AN ALGEBRAIC VARIETY AND AUTOMORPHIC FUNCTIONS

by Goro Shimura

One of our colleagues asked me not to release the "latest" pictures in this conference, but to rerun some classical ones. Following his suggestion, at least in the first half of this lecture, I will tell the old story of what happened to the zeta-function of an algebraic curve uniformized by modular functions. Then I'd like to talk about its application to the law of reciprocity in non-solvable extensions, and indicate briefly some generalization.

1. Introduction. Let $V$ be an algebraic variety defined over an algebraic number field $k$. For every prime ideal $\mathfrak{p}$ of $k$, let $V(\mathfrak{p})$ denote the reduction of $V$ modulo $\mathfrak{p}$ and $k(\mathfrak{p})$ the residue field of $k$ modulo $\mathfrak{p}$. For each $\mathfrak{p}$, we can define the zeta-function $Z(u; V(\mathfrak{p})/k(\mathfrak{p}))$ by

$$Z(0; V(\mathfrak{p})/k(\mathfrak{p})) = 1, \quad d[\log Z(u; V(\mathfrak{p})/k(\mathfrak{p}))] = \sum_{m=1}^{\infty} N_m u^{m-1} du$$

where $N_m$ is the number of points on $V(\mathfrak{p})$ rational over the extension of $k(\mathfrak{p})$ of degree $m$. The zeta-function of $V$ over $k$, denoted by $\zeta(s; V/k)$, is then defined by

$$\zeta(s; V/k) = \prod_{\mathfrak{p}} Z(N(\mathfrak{p})^{-s}; V(\mathfrak{p})/k(\mathfrak{p})),$$

the product being taken over all the prime ideals $\mathfrak{p}$ of $k$. If we assume Weil's conjecture to be true for $V$, then, for all except a finite number of $\mathfrak{p}$, $Z(u; V(\mathfrak{p})/k(\mathfrak{p}))$ can be written in the form

$$Z(u; V(\mathfrak{p})/k(\mathfrak{p})) = \frac{H_{\mathfrak{p}}^{(1)}(u) \cdots H_{\mathfrak{p}}^{(2n-1)}(u)}{H_{\mathfrak{p}}^{(0)}(u) \cdots H_{\mathfrak{p}}^{(2n)}(u)} .$$

Here $n = \dim(V)$; and $H_{\mathfrak{p}}^{(i)}(u)$ is a polynomial, with the constant term 1, whose roots are algebraic integers of absolute value $N(\mathfrak{p})^{-i/2}$. Moreover we may expect that the degree of $H_{\mathfrak{p}}^{(i)}$ is independent of $\mathfrak{p}$ for each $i$. Then it will be meaningful to consider a function

$$\zeta^{(i)}(s; V/k) = \prod_{\mathfrak{p}}' H_{\mathfrak{p}}^{(i)}(N(\mathfrak{p})^{-s}),$$

where the product is taken over all good $\mathfrak{p}$'s. Now the conjecture of Hasse - Weil (in the generalized sense) may be stated as follows: For every $i$, $\zeta^{(i)}(s; V/k)$ is meromorphically continued on the whole $s$-plane and satisfies a functional equation. For example, if $V$ is an abelian variety (resp. a curve), one has

$$\zeta^{(1)}(s; V/k) = \prod_{\mathfrak{p}}' \det[1 - M_{\ell}(\pi_{\mathfrak{p}})\, N(\mathfrak{p})^{-s}],$$

where $\pi_{\mathfrak{p}}$ is the $N(\mathfrak{p})$-th power endomorphism of $V(\mathfrak{p})$ (resp. the jacobian of $V(\mathfrak{p})$), and $M_{\ell}(\pi_{\mathfrak{p}})$ is its $\ell$-adic representation. Therefore, the determination of $\zeta^{(1)}(s; V/k)$ is, roughly speaking, the determination of $M_{\ell}(\pi_{\mathfrak{p}})$ as a function of $\mathfrak{p}$.

At present, there are two known classes of varieties $V$ for which the Hasse - Weil conjecture is true:

(I) abelian varieties with sufficiently many complex multiplications;

(II) algebraic curves uniformized by certain automorphic functions of one variable.

In the case (I), $V$ is an abelian variety of dimension $n$ such that $\mathrm{End}_{\mathbf{Q}}(V)$ is isomorphic to an algebraic number field $F$ of degree $2n$.[1]

---

1 One may consider a somewhat more general case where $\mathrm{End}_{\mathbf{Q}}(V)$ is not necessarily a field. For simplicity, we assume here $\mathrm{End}_{\mathbf{Q}}(V)$ to be a field.

It can be shown that there exists an element $\mu_p$ in $\mathrm{End}_Q(V)$ whose reduction modulo $p$ is $\pi_p$. Moreover, one can determine the prime ideal-decomposition of $(\mu_p)$ in $F$. These facts, together with a simple class-field theoretical consideration, show that $p \to \mu_p$ is essentially a Größen-character of $k$. From this it follows that $\zeta^{(1)}(s; V/k)$ is a product of $2n$ Hecke's $L$-functions with Größen-characters. Detailed accounts of the theory, and partial or related results can be found in Taniyama [17], Deuring [1], Weil [18]; a comparatively easy and short description is given also in [14, Ch. IV, § 18].

Among many factors which make the calculation of $\zeta^{(1)}$ possible in the case (I), it is most important that $\pi_p$ can be lifted up to an element of $\mathrm{End}_Q(V)$ for every $p$. Of course we can not expect this in general. However, in the case (II), we can show, roughly speaking, that $\pi_p + \pi_p^*$ belongs to the original $\mathrm{End}_Q(V)$ for a certain involution $*$. This fact makes it possible to prove the Hasse-Weil conjecture for the curves of (II). To explain this in detail, we need some preliminaries on automorphic forms and Hecke operators.

2. Discontinuous groups and automorphic forms on the upper half plane.

Let $H$ be the complex upper half plane, i.e.,

$$H = \{ z \in C \mid \mathrm{Im}(z) > 0 \}.$$

Every $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R)$ with $\det(\alpha) > 0$ acts on $H$ by $\alpha(z) = (az + b)/(cz + d)$. $H$ has a measure invariant under this action. A discrete subgroup $\Gamma$ of $SL_2(R)$ is called a Fuchsian group of the first kind, if $H/\Gamma$ is of finite measure. Hereafter we fix such a $\Gamma$. An element

$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $\Gamma$, other than $\pm 1$, is called <u>parabolic</u> if $z \to (az+b)/(cz+d$ has only one fixed point on the whole $z$-sphere. If that is so, the fixed point should be a real number or the point at infinity, and is called a <u>cusp</u> of $\Gamma$. Let $s$ be a cusp of $\Gamma$. All the elements of $\Gamma$ which leave $s$ invariant ar parabolic. Together with $\pm 1$, they form a group which is the product of $\{\pm 1\}$ and an infinite cyclic group generated by an element $\tau$ of the form $\tau = \rho \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rho^{-1}$ with an element $\rho$ of $SL_2(R)$ such that $\rho(\infty) = s$. Let $H^*$ be the union of $H$ and all the cusps of $\Gamma$. We can introduce a complex structure $H^*/\Gamma$ so that $H^*/\Gamma$ is a compact Riemann surface. To be more precise, a base of neighborhoods of $s$ in $H^*$ is given by $\rho(\{ z \in C \mid \mathrm{Im}(z) > r \})$ for $r > 0$, and $\exp[2\pi i \rho^{-1}(z)]$ is a local analytic coordinate around $s$ modulo $\Gamma$. Therefore $H/\Gamma$ is compact if and only if $\Gamma$ has no parabolic elements.

For every $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R)$ with $\det(\alpha) > 0$, set

$$j(\alpha, z) = \det(\alpha)^{1/2} (cz+d)^{-1}.$$

We can verify easily $j(\alpha, z)^2 = (d/dz)\alpha(z)$, and

$$j(\alpha\beta, z) = j(\alpha, \beta(z)) j(\beta, z).$$

Let $m$ be an integer. An <u>automorphic form of weight</u> $m$ <u>with respect to</u> $\Gamma$ is a meromorphic function $f$ on $H$ satisfying the following conditions (A1, 2).

(A1) $\quad f(\alpha(z)) j(\alpha, z)^m = f(z)$ <u>for every</u> $\alpha \in \Gamma$.

To describe the condition (A2), take a cusp $s$ of $\Gamma$ and elements $\tau, \rho$ of $GL_2(R)$ as above. If $f$ satisfies (A1), the function $f(\rho(z)) j(\rho, z)^m$ is invariant under the translation $z \to z+1$. Hence there exists a function

$F_s(q)$, meromorphic in $0 < |q| < 1$, such that $f(\rho(z))\,j(\rho,z)^m = F_s(e^{2\pi iz})$. Then (A2) is stated as follows:

(A2) *For every cusp* $s$ *of* $\Gamma$, $F_s(q)$ *is meromorphic at* $q = 0$.

An automorphic form of weight 0 is called an *automorphic function*. If $g$ is a meromorphic function on the compact Riemann surface $H^*/\Gamma$ and $\varphi$ is a natural projection of $H^*$ to $H^*/\Gamma$, then $g \circ \varphi$ is an automorphic function with respect to $\Gamma$; conversely, every automorphic function with respect to $\Gamma$ can be obtained in this way.

An automorphic form $f$ of weight $m > 0$ is called a *cusp form* if $f$ is holomorphic on the whole $H$, and the following condition is satisfied:

(A3) *For every cusp* $s$ *of* $\Gamma$, $F_s(q)$ *is holomorphic* at $q = 0$.

We denote by $S_m(\Gamma)$ the set of all cusp forms of weight $m$ with respect to $\Gamma$. The dimension of $S_m(\Gamma)$ can be determined easily by means of the Riemann - Roch theorem for $H^*/\Gamma$. In particular, there is a canonical isomorphism $f \longrightarrow \omega$ of $S_2(\Gamma)$ onto the vector space of all the differential forms of the first kind on $H^*/\Gamma$, defined by $\omega \circ \varphi = f(z)\,dz$. Therefore the dimension of $S_2(\Gamma)$ over $C$ is exactly the genus of $H^*/\Gamma$.

3. *Hecke operators*. Let $\Delta$ be the subset of $GL_2(R)$, closed under multiplication, and containing $\Gamma$. Suppose that $\det(\alpha) > 0$ for every $\alpha \in \Delta$, and the following condition is satisfied:

(3.1) *For every* $\alpha \in \Delta$, *the double coset* $\Gamma\alpha\Gamma$ *contains only a finite number of right and left cosets with respect to* $\Gamma$.

Let $R(\Gamma,\Delta)$ be the module consisting of all the formal finite sums $\sum_\lambda c_\lambda \Gamma\alpha_\lambda\Gamma$ with $\alpha_\lambda \in \Delta$, $c_\lambda \in C$. We can introduce a law of multiplicatior

in $R(\Gamma,\Delta)$ as follows. Let $\alpha,\beta\in\Delta$, and let $\Gamma\alpha\Gamma=\cup_i\Gamma\alpha_i$ and $\Gamma\beta\Gamma=\cup_j\Gamma\beta_j$ be disjoint expressions. Then for every $\Gamma\xi\Gamma$ with $\xi\in\Delta$, the number of $(i,j)$ such that $\Gamma\alpha_i\beta_j=\Gamma\xi$ is uniquely determined by the double cosets $\Gamma\alpha\Gamma$, $\Gamma\beta\Gamma$, $\Gamma\xi\Gamma$; it is independent of the choice of representatives $\{\alpha_i\},\{\beta_j\},\xi$. Call this number $\mu(\Gamma\alpha\Gamma\cdot\Gamma\beta\Gamma;\Gamma\xi\Gamma)$ and set

$$(3.2)\qquad \Gamma\alpha\Gamma\cdot\Gamma\beta\Gamma=\sum_{\Gamma\xi\Gamma}\mu(\Gamma\alpha\Gamma\cdot\Gamma\beta\Gamma;\Gamma\xi\Gamma)\Gamma\xi\Gamma.$$

Extending this to the whole $R(\Gamma,\Delta)$ by linearity, we get an associative ring.

Every element of $R(\Gamma,\Delta)$ operates on $S_m(\Gamma)$ in the following way: Let $\Gamma\alpha\Gamma=\cup_{i=1}^{d}\Gamma\alpha_i$ be a disjoint expression. For every $f\in S_m(\Gamma)$, define $g=f|T_m(\Gamma\alpha\Gamma)$ by

$$g(z)=\det(\alpha)^{m/2-1}\sum_{i=1}^{d}f(\alpha_i(z))\,j(\alpha_i,z)^{-m}.$$

It can easily be shown that $g\in S_m(\Gamma)$. In view of (3.2), we see that $\Gamma\alpha\Gamma\to T_m(\Gamma\alpha\Gamma)$ defines a representation of $R(\Gamma,\Delta)$ by linear transformations in $S_m(\Gamma)$.

Let us now consider a special case where $\Gamma$ is $SL_2(Z)$, and $\Delta$ is the set of all integral matrices of size 2 and with positive determinant. It can be shown that $R(\Gamma,\Delta)$ is a commutative integral domain. The representatives for $\Gamma\backslash\Delta/\Gamma$ are given by the matrices of the form $\alpha=\begin{pmatrix}a&0\\0&d\end{pmatrix}$, where $a>0$ and $a$ divides $d$. For this $\alpha$, let $T(a,d)$ denote $\Gamma\alpha\Gamma$ (as an element of $R(\Gamma,\Delta)$). Then we have

$$(3.3)\qquad T(a,d)\,T(a',d')=T(aa',dd')\quad\text{if}\quad(d,d')=1.$$

Therefore $R(\Gamma,\Delta)$ is generated by the $T(p^\lambda,p^\mu)$ with $\mu\geq\lambda\geq 0$ for all the prime numbers $p$. Let $T(p^n)$ be the sum of all $T(p^\lambda,p^\mu)$ such that

$\lambda + \mu = n$, $\mu \geq \lambda \geq 0$. Then we can prove that

$$T(p)\,T(p^n) = T(p^{n+1}) + pT(p,p)\,T(p^{n-1}) \qquad (n > 0).$$

From this it follows that, $u$ being an indeterminate,

$$(3.4) \qquad \sum_{n=1}^{\infty} T(p^n)u^n = [\,1 - T(p)u + pT(p,p)u^2\,]^{-1}.$$

Now we consider a formal Dirichlet series $D(s;\Gamma)$ with coefficients in $R(\Gamma,\Delta)$:

$$D(s;\Gamma) = \sum_{\Gamma\backslash\Delta/\Gamma} (\Gamma\alpha\Gamma)\det(\alpha)^{-s} = \sum_{a|d} T(a,d)(ad)^{-s},$$

where the sum is extended over all the double cosets $\Gamma\alpha\Gamma$ with $\alpha \in \Delta$. By virtue of (3.3) and (3.4), we get an Euler product:

$$D(s;\Gamma) = \prod_p [\,1 - T(p)p^{-s} + T(p,p)p^{1-2s}\,]^{-1}.$$

Let us define <u>the principal congruence subgroup</u> $\Gamma_N$ <u>of level</u> $N$ by

$$(3.5) \qquad \Gamma_N = \{\alpha \in SL_2(\mathbb{Z}) \mid \alpha \equiv I \bmod (N)\},$$

for every positive integer $N$. An automorphic form (resp. function) with respect to $\Gamma_N$ is usually called a <u>modular form</u> (resp. <u>function</u>) <u>of level</u> $N$. Let $\Delta_N$ be the set of all matrices $\alpha$ in $\Delta$ such that

$$\alpha \equiv \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \bmod (N), \quad (d, N) = 1,$$

and let $\Delta_N^*$ be the set of all $\alpha$ in $\Delta$ such that $(\det(\alpha), N) = 1$. Then we obtain an isomorphism of $R(\Gamma_N,\Delta_N)$ onto $R(\Gamma,\Delta_N^*)$ by

$$(3.6) \qquad \Gamma_N\alpha\Gamma_N \to \Gamma\alpha\Gamma \qquad (\alpha \in \Delta_N).$$

Therefore, if we set $D^N(s) = \sum_{\Gamma_N\backslash\Delta/\Gamma_N} (\Gamma_N\alpha\Gamma_N)\det(\alpha)^{-s}$, then

$$D^N(s) = \prod_{p\nmid N} [\,1 - T^N(p)p^{-s} + T^N(p,p)p^{1-2s}\,]^{-1},$$

where $T^N(p)$ and $T^N(p,p)$ are the elements of $R(\Gamma_N,\Delta_N)$ corresponding to $T(p)$ and $T(p,p)$ by the isomorphism (3.6), respectively.

Taking the representation in $S_m(\Gamma_N)$: $\Gamma_N\alpha\Gamma_N \to T_m(\Gamma_N\alpha\Gamma_N)$, we

get a Dirichlet series with matrix coefficients

$$(3.7)\qquad D_m^N(s) = \sum_{\Gamma_N\backslash\Delta/\Gamma_N} T_m(\Gamma_N\alpha\Gamma_N)\det(\alpha)^{-s}$$

$$= \prod_{p\nmid N}\left[1 - T_m^N(p)p^{-s} + T_m^N(p,p)p^{1-2s}\right]^{-1},$$

which converges absolutely for suitably large $\mathrm{Re}(s)$. Moreover, $D_m^N(s)$ can be continued holomorphically on the whole complex $s$-plane and satisfies a functional equation. If $N=1$, the functional equation has the following form:

$$D_m^*(s) = D_m^*(m-s) \quad \text{with} \quad D_m^*(s) = \Gamma(s)(2\pi)^{-s}D_m^1(s).$$

With respect to a suitable basis $\{f_1, \ldots, f_h\}$ of $S_m(\Gamma_1)$, the $T_m(\Gamma_1\alpha\Gamma_1)$ can be represented by diagonal matrices simultaneously. At the cusp $\infty$ of $\Gamma_1$, each form $f_j$ has a Fourier expansion

$$f_j(z) = \sum_{n=1}^{\infty} a_n(j)\, e^{2\pi i n z}.$$

Then one can prove that the diagonal elements of $D_m^1(s)$ are

$$\sum_{n=1}^{\infty} a_n(j)\, n^{-s} = \prod_p \left[1 - a_p(j)\, p^{-s} + p^{m-1-2s}\right]^{-1}$$

$$(1 \leqq j \leqq h).$$

In particular, $S_{12}(\Gamma_1)$ is one-dimensional and generated by

$$(3.8)\qquad \Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty} a_n q^n, \quad q = e^{2\pi i z}.$$

In 1916, Ramanujan conjectured the existence of Euler product for $\sum_{n=1}^{\infty} a_n n^{-s}$ with the coefficients $a_n$ of (3.8) and the inequality $|a_p| < 2p^{11/2}$ for every prime number $p$. The Euler product was established by Mordell. In [3, 4], Hecke completed a general theory of constructing Dirichlet series with Euler product and functional equation out of modular forms. The operators $T_m(\Gamma\alpha\Gamma)$ are called Hecke operators. This work was followed by Petersson who generalized Ramanujan's conjecture in the following form: "For every prime number $p$ not dividing $N$, the

characteristic roots of $T_m^N(p)$ have absolute values $\leq 2p^{(m-1)/2}$." In the above, I gave a survey of (a part of) Hecke's result. For the formulation of $R(\Gamma, \Delta)$ and its generalization, I refer to [11, 12, 13] and Tamagawa [15, 16].

4. Modular correspondences and their congruence relations. Let $\Gamma$ be a Fuchsian group of the first kind, and $V$ a projective non-singular curve analytically isomorphic to $H^*/\Gamma$. Let $\Delta$ be as in the beginning of § 3. Denote by $\varphi$ the natural projection of $H^*$ to $V$. Let $\alpha \in \Delta$, and let $X = \{\varphi(z) \times \varphi(\alpha(z)) \mid z \in H^*\}$. It can be shown that $X$ is a curve on $V \times V$, and if $\Gamma\alpha\Gamma = \bigcup_{i=1}^{d} \Gamma\alpha_i$ is a disjoint union, one has

$$X \cdot (\varphi(z) \times V) = \varphi(z) \times \sum_{i=1}^{d} \varphi(\alpha_i(z)). \tag{4.1}$$

In view of our definition (3.2) of the law of multiplication in $R(\Gamma, \Delta)$, we see that $\Gamma\alpha\Gamma \longrightarrow X$ defines a homomorphism of $R(\Gamma, \Delta)$ into the ring of algebraic correspondences of $V$. We call $X$ a modular correspondence of $V$.

Now let us take the group $\Gamma_N$ defined by (3.5) as our $\Gamma$. Let $V_N$ be a projective non-singular model for $H^*/\Gamma_N$, and $X_p^N$, $Y_p^N$ be the modular correspondences of $V_N$ obtained from the elements $T^N(p)$, $T^N(p, p)$ of $R(\Gamma_N, \Delta_N)$, respectively.

Theorem: A model $V_N$ for $H^*/\Gamma_N$ can be taken so that $V_N$, $X_p^N$, $Y_p^N$ are defined over $Q$, and, for all but a finite number of $p$,

$$(X_p^N)_p = \prod_p + \prod_p' \circ (Y_p^N)_p,$$

$$\prod_p' \circ (Y_p^N)_p = (Z)_p^{-1} \circ \prod_p' \circ (Z)_p \text{ on } (V_N \times V_N)_p.$$

Here $(\ )_p$ means reduction modulo $p$, $\prod_p$ is the locus of $x \times x^p$ on

$(V_N \times V_N)_p$, *i.e., the Frobenius correspondence,* $\prod_p'$ *is the transpose of* $\prod_p$, *and* $Z$ *is a certain birational automorphism of* $V_N$ *independent of* $p$

We shall sketch the proof in the following section.

Let $J_N$ be the jacobian variety of $V_N$, and let $\xi_p, \eta_p, \zeta$ be the elements of $\mathrm{End}(J_N)$ corresponding to $X_p, Y_p, Z$. From our theorem it follows easily that

$$(\xi_p)_p = \pi_p + \pi_p' \circ (\eta_p)_p, \tag{4.3}$$

$$\pi_p^{\dagger} \circ (\eta_p)_p = (\zeta)_p^{-1} \cdot \pi_p' \circ (\zeta)_p. \tag{4.4}$$

On $J_N$ and $(J_N)_p$, we can find $\ell$-adic coordinate systems so that $M_\ell(\lambda) = M_\ell((\lambda)_p)$ for every $\lambda$ of $\mathrm{End}(J_N)$ defined over $Q$. Then, $u$ being an indeterminate, from (4.3) and (4.4) we obtain

$$\det[1 - M_\ell(\xi_p)u + M_\ell(\eta_p)pu^2] = \det[1 - M_\ell(\pi_p)u]^2. \tag{4.5}$$

Let $M^d(\lambda)$ be a representation of $\lambda \in \mathrm{End}(J_N)$ in $H^{1,0}(J_N)$. It is well known that $M_\ell$ is equivalent to the direct sum of $M^d$ and its complex conjugate. Since $\xi_p$ and $\eta_p$ are defined over $Q$, we may assume that $M^d(\xi_p)$ and $M^d(\eta_p)$ have rational coefficients, so that

$$\det[1 - M^d(\xi_p)u + M^d(\eta_p)pu^2] = \det[1 - M_\ell(\pi_p)u].$$

Now $\xi_p$ (resp. $\eta_p$) corresponds to $X_p$ (resp. $Y_p$), and $X_p$ (resp. $Y_p$) is obtained from $T^N(p)$ (resp. $T^N(p,p)$). As remarked at the end of §2, $S_2(\Gamma_N)$ is canonically isomorphic to $H^{1,0}(V_N)$. Therefore $M^d(\xi_p)$ and $M^d(\eta_p)$ are essentially the same as $T_2^N(p)$ and $T_2^N(p,p)$. We get hence

$$\det[1 - M_\ell(\pi_p)p^{-s}] = \det[1 - T_2^N(p)p^{-s} + T_2^N(p,p)p^{1-2s}].$$

The right hand side is exactly the determinant of the inverse of the $p$-factor of the Euler product (3.7) for $m = 2$. We have thus proved that

$\zeta^{(1)}(s, V_N/Q)$ is equal to $\det[D_2^N(s)]^{-1}$ up to a finite number of p-factors. Therefore the Hasse-Weil conjecture is assured for the curve $V_N$.

Combining (4.3) with Weil's result which asserts that the characteristic roots of $M_\ell(\mathfrak{r}_p)$ have the absolute value $p^{1/2}$, we know that the characteristic roots of $T_2^N(p)$ have absolute values not greater than $2p^{1/2}$ for almost all p.

5. Proof of the congruence relation. Let $g_2(\omega_1, \omega_2), g_3(\omega_1, \omega_2), P(x; \omega_1, \omega_2)$ be the functions of complex variables $\omega_1, \omega_2, x$ with the condition $\mathrm{Im}(\omega_1/\omega_2) > 0$, defined by

$$g_2(\omega_1, \omega_2) = 60\sum{}' \omega^{-4}, \quad g_3(\omega_1, \omega_2) = 140\sum{}' \omega^{-6},$$

$$P(x; \omega_1, \omega_2) = x^{-2} + \sum{}'[(x-\omega)^{-2} - \omega^{-2}],$$

where $\sum'$ means the sum extended over all the elements $\omega$, other than 0, of the module $Z\omega_1 + Z\omega_2$. Define functions $j(z)$ and $f_{ab}^N(z)$ on H by

$$z = \omega_1/\omega_2,$$

$$j(z) = g_2(\omega_1, \omega_2)^3/[g_2(\omega_1, \omega_2)^3 - 27g_3(\omega_1, \omega_2)^2],$$

$$f_{ab}^N(z) = g_2(\omega_1, \omega_3)\, g_3(\omega_1, \omega_3)^{-1} P((a\omega_1 + b\omega_2)/N; \omega_1, \omega_2)$$

$$(a, b \in Z; (a, b) \not\equiv (0, 0) \bmod (N));$$

It is well known that $C(j)$ is the field of all modular functions of level 1. By a simple calculation, we observe that for every $\alpha \in \Gamma_1$,

$$\left[f_{ab}^N(\alpha(z)) = f_{ab}^N(z) \text{ for all } (a, b)\right] \Leftrightarrow \pm\alpha \in \Gamma_N.$$

From this it follows that all the $f_{ab}^N$ and $j$ generate the field of all modular functions of level N.

Roughly speaking, the modular functions of level N are obtained from the invariant of elliptic curves and points of finite order on the curves. To be more precise, for $z \in H$, determine $\gamma$ by $j(z) = \gamma/(\gamma - 27)$ and call

$E(z)$ the elliptic curve $y^2 = 4x^3 - \gamma_2 x - \gamma_3$. Then $E(z)$ has the invariant $j(z)$. Let $h_z$ be the function on $E(z)$ such that $h_z(x, y) = x$ for $(x, y) \in E(z)$. Let us fix a point $z_0$ such that $j(z_0)$ is transcendental over $Q$, and set $j_0 = j(z_0)$, $E_0 = E(z_0)$, $h_0 = h_{z_0}$,

$$K_N = Q(j_0, h_0(t) \mid t \in E_0, \ Nt = 0).$$

Then the field $K_N$ is isomorphic to $Q(j, f_{ab}^N)$. Moreover, $K_N$ is a Galois extension of $Q(j_0)$, and the Galois group is isomorphic to $GL_2(Z/NZ)/\{\pm 1\}$. Let $L_N$ be the subfield of $K_N$ corresponding to the subgroup $\{\pm \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid (a, N) = 1\}/\{\pm 1\}$. Then $L_N(e^{2\pi i/N}) = K_N$, and $L_N$ has $Q$ as its constant field. Therefore, if we take a curve $V_N$ whose function-field over $Q$ is $L_N$, then $V_N$ is a model for $H^*/\Gamma_N$ and actually defined over $Q$.

Now let us consider a disjoint expression

$$T^N(p) = \Gamma_N \alpha \Gamma_N = \bigcup_{i=1}^{p+1} \Gamma_N \alpha_i \quad \text{with} \quad \alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$$

for a prime number $p$ not dividing $N$. Set $z_i = \alpha_i(z)$, $j_i = j(z_i)$, $E_i = E(z_i)$, $h_i = h_{z_i}$ for $1 \leq i \leq p+1$. Since $\det(\alpha_i) = p$, one can find an isogeny $\lambda_i$ of $E_i$ to $E_1$ whose kernel is of order $p$. Then the $\mathrm{Ker}(\lambda_i)$ for $1 \leq i \leq p+1$ are exactly all the subgroups of order $p$ of $E_0$. In view of (4.1), the modular correspondence $X_p^N$ can be described by the mapping

$$(j(z_0), f_{ab}^N(z_0)) \longrightarrow \{(j(z_i), f_{ab}^N(z_i)) \mid 1 \leq i \leq p+1\},$$

or

$$(5.1) \qquad (j_0, h_0(t)) \longrightarrow \{(j_i, h_i(\lambda_i t)) \mid 1 \leq i \leq p+1\},$$

where $t \in E_0$, $Nt = 0$. In this way $X_p^N$ may be connected with the isogenies of elliptic curves.

In the next place, we extend $(\mathfrak{p})$ to a prime divisor $\mathfrak{P}$ of a suitably large field containing $j_0, j_1$, etc., so that $\mathfrak{P}(j_0)$ is transcendental over $Z/pZ$. Let $(\ )_{\mathfrak{P}}$ mean reduction modulo $\mathfrak{P}$. Since $(E_0)_{\mathfrak{P}}$ has exactly $p$ points of order $p$, we have $(\mathrm{Ker}(\lambda_i))_{\mathfrak{P}} = \{0\}$ for exactly one $i$, say $i = 1$. Then $(\mathrm{Ker}(\lambda_i))_{\mathfrak{P}}$ is of order $p$ for $i > 1$. Hence $(\lambda_1)_{\mathfrak{P}}$ is a purely inseparable isogeny of degree $p$. It follows easily that $(E_1)_{\mathfrak{P}} = (E_0)_{\mathfrak{P}}^{p}$, and hence

$$(5.2) \qquad j \equiv j_0^{p}, \quad h_1(\lambda_1 t) \equiv h_0(t)^{p} \bmod \mathfrak{P} \quad (t \in E_0, \ Nt = 0).$$

Let $\mu_i$ be an isogeny of $E_i$ to $E_0$ such that $\mu_i \lambda_i = p$. Then we see that for $i > 1$, $\mu_i$ is purely inseparable, so that $(E_0)_{\mathfrak{P}} = (E_i)_{\mathfrak{P}}^{p}$,

$$(5.3) \qquad j_0 \equiv j_i^{p}, \quad h_0(\mu_i t) \equiv h_i(s)^{p} \bmod \mathfrak{P} \quad (s \in E, \ Ns = 0).$$

Substituting $\lambda_i t$ for $s$ in (5.3), we get

$$(5.4) \qquad j_i \equiv j_0^{1/p}, \quad h_i(\lambda_i t) \equiv h_0(pt)^{1/p} \bmod \mathfrak{P} \quad (i > 1: t \in E_0, \ Nt = 0).$$

By (5.2) and (5.4), reduction modulo $\mathfrak{P}$ of (5.1) is

$$(5.5) \qquad (j_0, h_0(t))_{\mathfrak{P}} \to (j_0^{p}, h_0(t)^{p})_{\mathfrak{P}} + p \text{ times } (j_0^{1/p}, h_0(pt)^{1/p})_{\mathfrak{P}} \quad (t \in E_0, \ Nt = 0).$$

It can be shown that the operation $(j_0, h_0(t)) \to (j_0, h_0(pt))$ gives exactly $Y_p^N$ on $V_N$. Therefore from (5.5) we obtain $(X_p^N)_{\mathfrak{P}} = \prod_{\mathfrak{P}} + \prod_{\mathfrak{P}}' + (Y_p^N)_{\mathfrak{P}}$.

The first relation in our theorem was found by Eichler [2] for a certain field of modular functions with respect to the group

$$(5.6) \qquad \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z) \mid c \equiv 0 \bmod (N) \right\}.$$

The result was generalized by [10], whose method I followed in the above. The result for $\Gamma_0(N)$ or any congruence subgroup of $\Gamma_1$ is derivable

essentially from the result for $\Gamma_N$. However, as we shall see later, it is convenient to state the result for some particular congruence subgroups such as $\Gamma_0(N)$. For detail I refer to [2, 10]. Now Igusa [6] showed that the reduction process works well for all primes $p$ not dividing $N$. This fact is useful in our later discussion.

6. The unit group of a quaternion algebra. Let $\mathfrak{H}$ be an indefinite quaternion algebra over $Q$, i.e., an algebra such that $\mathfrak{H} \otimes_Q R$ is isomorphic to the total matrix algebra $M_2(R)$. Let $\mathfrak{o}$ be a maximal order in $\mathfrak{H}$, i.e., a maximal one among the subrings of $\mathfrak{H}$ which are finitely generated modules over $Z$. We consider $\mathfrak{H}$ as a subring of $M_2(R)$, and set

$$\Gamma(\mathfrak{o}) = \{\alpha \in \mathfrak{o} \mid \det(\alpha) = 1\},$$

$$\Gamma_N(\mathfrak{o}) = \{\alpha \in \Gamma(\mathfrak{o}) \mid \alpha \equiv 1 \bmod N\},$$

where $N$ is any positive integer. Then the groups $\Gamma(\mathfrak{o})$ and $\Gamma_N(\mathfrak{o})$, regarded as subgroups of $SL_2(R)$, are Fuchsian groups of the first kind. If $\mathfrak{H} = M_2(Q)$, these are nothing but $\Gamma_1$ and $\Gamma_N$ considered in § 3. If $\mathfrak{H}$ is a division algebra, they have compact quotient spaces.

Suppose that $N$ is prime to the discriminant of $\mathfrak{H}$. Then the ring $\mathfrak{o}/N\mathfrak{o}$ may be identified with the matrix ring $M_2(Z/NZ)$. Let $\Delta_N(\mathfrak{o})$ be the set of elements $\alpha$ in $\mathfrak{o}$ such that $\det(\alpha) > 0$, $\alpha \equiv \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \bmod N\mathfrak{o}$. Then we can show that $R(\Gamma_N(\mathfrak{o}), \Delta_N(\mathfrak{o}))$ has the same structure as $R(\Gamma_N, \Delta_N)$ of § 3. Taking the representation of $R(\Gamma_N(\mathfrak{o}), \Delta_N(\sigma))$ in $S_m(\Gamma_N(\mathfrak{o}))$, we can construct a Dirichlet series $D_m^N(s; \mathfrak{H})$ with a functional equation and an Euler product analogous to (3.7). Furthermore, $H/\Gamma_N(\mathfrak{o})$ has a model $V_N(\mathfrak{o})$ defined over $Q$, provided that $N$ is prime

to the discriminant of $\Phi$; and $\zeta^{(1)}(s; V_N(\sigma)/\Omega)$ differs from $\det[D_2^N(s;\Phi)]^{-1}$ only by a finite number of p-factors.

This result can be proved as follows. First we define, for every $z \in H$, a complex torus $A_z$ of dimension 2 by

$$(6.1) \qquad A_z = C^2/L_z, \quad L_z = \{a\begin{pmatrix} z \\ 1 \end{pmatrix} \mid a \in \sigma\},$$

where an element of $\sigma$ is considered as an element of $M_2(R)$. One can prove that $A_z$ has a structure of abelian variety. Furthermore, every element of $\sigma$ defines an endomorphism of $A_z$ in a natural manner. Endowed with a suitable polarization, the $A_z$ form an analytic family $\{A_z \mid z \in H\}$ of abelian varieties with the structure of endomorphisms and polarization, parametrized by the points of $H$. The moduli of an abelian variety $A_z$ with such a structure are given by the values of automorphic functions with respect to $\Gamma(\sigma)$ at $z$. The automorphic functions with respect to the congruence subgroup $\Gamma_N(\sigma)$ can be obtained from the coordinates of the points of order $N$ on $A_z$. Here again we can connect Hecke operators (or modular correspondences on $H/\Gamma_N(\sigma)$) with the isogenies of $A_z$. Using the same idea as in § 5, we obtain congruence relations for modular correspondences on $H/\Gamma_N(\sigma)$, though the present case involves more technical difficulties than the case of elliptic modular functions. A full detail of the theory is given in [12].

7. A law of reciprocity in non-solvable extensions. Let us consider the group $\Gamma_0(N)$ of (5.6) for a particular case, $N = 11$. It is known [5] that $S_2(\Gamma_0(11))$ is one-dimensional and generated by

$$[\Delta(z)\Delta(11z)]^{1/12} = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 \qquad (q = e^{2\pi iz}).$$

Write this as $\sum_{n=1}^{\infty} c_n q^n$, and set $D(s) = \sum_{n=1}^{\infty} c_n n^{-s}$. By Hecke's theory we have

$$(7.1) \qquad D(s) = (1 - 11^{-s})^{-1} \prod_{p \neq 11} (1 - c_p p^{-s} + p^{1-2s})^{-1},$$

$$D^*(s) = D^*(2 - s) \quad \text{with} \quad D^*(s) = \Gamma(s)(2\pi)^{-s} 11^{s/2} D(s).$$

The field of automorphic functions with respect to $\Gamma_0(11)$ is generated by $j(z)$ and $j(11z)$; and $Q(j(z), j(11z))$ has a model

$$(7.2) \qquad E: y^2 = 4x^3 - (4 \cdot 31/3)x - (2501/27).$$

Therefore, by virtue of the congruence relation, we know that if $\pi_p$ is the $p$-th power endomorphism of $(E)_p$, then

$$(7.3) \qquad \det[X - M_\ell(\pi_p)] = X^2 - c_p X + p$$

with the $c_p$ determined by

$$(7.4) \qquad \sum_{n=1}^{\infty} c_n q^n = q \cdot \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2.$$

By the result of Igusa mentioned at the end of § 6, the relation (7.3) is true for <u>all</u> $p \neq 11$.

Let $\ell$ be a prime number, and $K_\ell$ the field generated over $Q$ by all the coordinates of the points of order $\ell$ on the elliptic curve $E$ (7.2) Then $K_\ell$ is a Galois extension of $Q$, and every element of the Galois group $G(K_\ell/Q)$ gives an automorphism of the group of points of order $\ell$ on $E$. Hence we obtain an isomorphism $S_\ell$ of $G(K_\ell/Q)$ into $GL_2(Z/\ell Z)$. Let $p$ be a prime number, other than 11 and $\ell$. Let $P$ be a prime ideal in $K_\ell$ dividing $p$, and $\sigma_p$ a Frobenius automorphism of $K_\ell$ over $Q$ for $P$. By taking suitable $\ell$-adic coordinate systems on $E$ and $(E)_p$, we find $S_\ell(\sigma_p) \equiv M_\ell(\pi_p) \bmod (\ell)$, so that

$$(7.5) \qquad \det[X - S_\ell(\sigma_p)] \equiv X^2 - c_p X + p \bmod (\ell).$$

It follows, in particular, that $S_\ell(G(K_\ell/Q))$ contains an element whose characteristic polynomial is $X^2 - c_p X + p$. Using this fact, I found that $S_\ell(G(K_\ell/Q)) = GL_2(Z/\ell Z)$ at least for $7 \leq \ell \leq 97$.

This fact is interesting, for there was previously no known example of non-solvable extension for which the law of reciprocity is given explicitly (in any sense); here are such examples. In fact, we have obtained a Galois extension $K_\ell$ of $Q$ whose Galois group is isomorphic to $GL_2(Z/\ell Z)$, and of which the law of reciprocity is given by (7.5), where the $c_p$ are coefficients of the Dirichlet series (7.1) with Euler product and functional equation; they are easily obtained from (7.4) as many as we need! Moreover, we can determine Artin's L-functions of the extension $K_\ell/Q$ for a fairly large number of characters which are not simple. A more detailed account of the result will be published elsewhere.

We may expect a result of the same kind for other congruence subgroups and also for the Fuchsian group discussed in § 6 (cf. [12, pp. 328-329]). But here my emphasis is laid on the explicitness or comprehensibility, and not on generality. It will be an important task to reorganize and generalize the result from a new view-point.

8. Change of model and extension of basic field. In the case of an abelian variety $A$ with sufficiently many complex multiplications, we can determine $\zeta^{(1)}(s; A/k)$ for almost any field of definition $k$ of $A$. Contrary to this, in the case of the curve $H^*/\Gamma_N$ (or $H/\Gamma_1(\ell)$), we have determined $\zeta^{(1)}(s; V_N/Q)$ only for a particular model $V_N$ over $Q$. It is not an easy problem to prove the Hasse-Weil conjecture for an arbitrary

model $V'$ birationally equivalent to $V_N$, with an arbitrary algebraic number field $k$ as the basic field. However, if $k$ is abelian over $Q$, a part of this problem may be solved in the following way. For every abelian character $\chi$ of $Q$, we define a Dirichlet series

$$D_m^N(s;\chi;\hat{\phi}) = \sum_{n=1}^{\infty} \chi(n) B_n n^{-s}$$

for $D_m^N(s;\hat{\phi}) = \sum_{n=1}^{\infty} B_n n^{-s}$. Then $D_m^N(s;\chi;\hat{\phi})$ can be continued holomorphically on the whole $s$-plane and satisfies a functional equation [13, Th. 1]. It is easy to see that $\zeta^{(1)}(s; V_N(\mathcal{O})/k)$ is a product of $\det[D_2^N(s;\chi;\hat{\phi})]^{-1}$ for several $\chi$'s, up to a finite number of $p$-factors. A discussion from a somewhat different view-point can be found in Rangachari [9], Konno [7].

As an explicit example, the $c_n$ being as in (7.1) and (7.4), set

$$D(s;\chi) = \sum_{n=1}^{\infty} \chi(n) c_n n^{-s},$$

$$D^*(s;\chi) = \Gamma(s)(2\pi)^{-s}(11d^2)^{s/2} D(s;\chi)$$

for a primitive character $\chi$ with the conductor $(d)$. Then one can prove

$$D^*(s;\chi) = \chi(11) W(\chi)^2 D^*(2-s;\overline{\chi}),$$

where $W(\chi) = |d|^{-1/2} \sum_{a=1}^{d} \chi(a) e^{2\pi i a/|d|}$, and $\overline{\chi}$ is the complex conjugate of $\chi$. In particular, if $\chi(n) = (\frac{d}{n})$ (Kronecker's symbol), one has $W(\chi)^2 = \chi(-1)$, so that

$$D^*(s;\chi) = \chi(-11) D^*(2-s;\chi).$$

Now let $E$ be defined by (7.2), and $E'$ an elliptic curve isomorphic to $E$ over $C$ but not isomorphic over $Q$. Since $\pm 1$ are only automorphisms of $E$, every isomorphism $\lambda$ of $E$ to $E'$ is defined over a quadratic extension $Q(\sqrt{d})$ for some $d \in Q$. Here we take as $d$ the

discriminant of $Q(\sqrt{d})$. Then it can be easily verified that $\zeta^{(1)}(s; E'/Q)$ is, up to a finite number of p-factors, equal to $D(s;\chi)^{-1}$ with $\chi(n) = (\frac{d}{n})$. Therefore, the Hasse-Weil conjecture for $E'$ over $Q$ is assured.

9. The zeta-function of a fibre variety. So far only automorphic forms of weight 2 have been related to the zeta-function of a curve. Now we can construct a certain fibre variety $W_N^{(h)}$ whose zeta-function is expressed by the Dirichlet series $D_m^N(s; \Phi)$ considered in § 6 for $m \geq 2$.

To construct such a fibre variety, take $\Phi$ and $\mathcal{O}$ as in § 6; assume that $\Phi$ is a division algebra. Let $GL_2^+(R)$ denote the group of elements in $GL_2(R)$ with positive determinant. For a positive integer $h$, let $F_h$ be the product of $h$ copies of $M_2(R)$, viewed as a right and left $M_2(R)$-module in a natural manner. The product $GL_2^+(R) \times F_h$ forms a group with respect to the law of multiplication:

$$(\xi, u)(\eta, v) = (\xi\eta, v\xi' + u) \qquad (\xi, \eta \in GL_2^+(R);\ u, v \in F_h)$$

where prime means a canonical involution of $M_2(R)$. We let $GL_2^+(R) \times F_h$ act on $H \times F_h$ by the rule:

$$(\alpha, u)(z, v) = (\alpha(z), v\alpha' + u) \qquad (\alpha \in GL_2^+(R);\ u, v \in F_h;\ z \in H).$$

Define a mapping $x_h$ of $H \times F_h$ onto $H \times C^{2h}$ by

$$x_h(z, u_1, \ldots, u_h) = (z, u_1\begin{pmatrix} z \\ 1 \end{pmatrix}, \ldots, u_h\begin{pmatrix} z \\ 1 \end{pmatrix})$$
$$(z \in H;\ u_i \in M_2(R)).$$

We introduce a complex structure in $H \times F_h$ so that $x_h$ is a complex analytic isomorphism. Then every element of $GL_2^+(R) \times F_h$ acts on $H \times F_h$ as a complex analytic automorphism.

Let $\sigma^h$ denote the product of $h$ copies of $\sigma$. As a subgroup of $GL_2^+(R) \times F_h$, $\Gamma_N(e) \times \sigma^h$ gives a properly discontinuous group of transformations on $H \times F_h$ with a compact quotient. Set

$$W_N^{(h)} = (\Gamma_N(e) \times \sigma^h) \backslash (H \times F_h).$$

Assume hereafter that $\Gamma_N(\sigma)$ has no element of finite order other than the identity element. Then $W_N^{(h)}$ is a compact complex manifold. Furthermore, one can easily verify that $W_N^{(h)}$ is a fibre variety of which the base is $V_N = \Gamma_N(e) \backslash H$, and each fibre is the product of $h$ copies of the abelian variety $A_z$ (6.1).

Kuga [8] determined completely the cohomology groups of a certain class of fibre varieties, which includes $W_N^{(h)}$ as a special case. In the case of $W_N^{(h)}$, it turns out that every cohomology group is canonically isomorphic to a direct sum of $S_m(\Gamma_N(\sigma))$ for some $m$'s. He proved also that $W_N^{(h)}$ can be embedded in a projective space.

Let $s \to w(s)$ be a natural projection of $H \times F_h$ to $W_N^{(h)}$. Assume that $N$ is prime to the discriminant of $\Phi$. Let $\Delta_N(\sigma)$ be as in § 6. For simplicity, set $\Gamma = \Gamma_N(\sigma)$, $\Delta = \Delta_N(\sigma)$. For every $\alpha \in \Delta$, set

$$X(\Gamma\alpha\Gamma) = \{ w(s) \times w(\{\alpha, 0\}s) \mid s \in H \times F_h \}.$$

We verify easily that $X$ is a subvariety of $W_N^{(h)} \times W_N^{(h)}$. It can be shown that $\Gamma\alpha\Gamma \to X(\Gamma\alpha\Gamma)$ defines an isomorphism of $R(\Gamma, \Delta)$ into the ring of correspondences on $W_N^{(h)}$, the latter being defined suitably.

One can find two elements $\alpha_p$ and $\beta_p$ of $\Delta$, for each prime number $p$, such that $\det(\alpha_p) = p$ and $p^{-1}\beta_p \in \Gamma(\sigma)$. Set

$$X_p^{(h)} = X(\Gamma\alpha_p\Gamma),\ Y_p^{(h)} = X(\Gamma\beta_p\Gamma).$$

Now we can find a projective model $W_N^{(h)}$ so that $W_N^{(h)}$, $X_p^{(h)}$, $Y_p^{(h)}$ are all defined over $Q$, and

$$(X_p^{(h)})_p = \prod_p + \prod_p^*,$$
$$p(Y_p^{(h)}) = \prod_p \circ \prod_p^*, \qquad \text{on } (W_N^{(h)} \times W_N^{(h)})_p$$

for all but a finite number of $p$. Here $(\ )_p$ means reduction modulo $p$, $\prod_p$ is the locus of $x \times x^p$ on $(W_N^{(h)} \times W_N^{(h)})_p$, $\prod_p^*$ is a certain correspondence such that $(\prod_p^*)^n$ has the same number of fixed points as $\prod_p^n$ for $n = 1, 2, \ldots$. Combining this congruence relation with the result of Kuga concerning the cohomology groups of $W_N^{(h)}$, mentioned above, we find

$$\zeta(s; W_N^{(h)}/Q) \doteq \prod_{b=0}^{4h} [\zeta(s-(b/2))\zeta(s-(b+2)/2)]^{e(h,b,0)}$$
$$\times \prod_{b=0}^{4h} \prod_{i=0}^{b} \det [D_{i+2}^N(s-(b-i)/2; \tilde{\phi})]^{e(h,b,i)(-1)^{b+i}},$$

where $\doteq$ means the equality up to a finite number of $p$-factors, and the $e(h,b,i)$ are non-negative integers, depending only on $h, b, i$. A full exposition of our result will appear as a collaboration with Kuga.

A formula of this kind was first given empirically by Sato for a certain fibre variety whose base is $H^*/\Gamma_N$ and fibres are the product of elliptic curves modulo $\pm 1$. A variety of this kind had been suggested by Kuga, as the one which would describe Ramanujan's function in terms of Hasse's zeta function.

## REFERENCES


1. M. Deuring, Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins I , II , III , IV , Nachr. Akad. Wiss. Göttingen, (1953) 85 - 94 , (1955) 13 - 42 , (1956) 37 - 76 , (1957) 55 - 80 .

2. M. Eichler, Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion, Arch. Math. 5(1954), 355 - 366 .

3. E. Hecke, Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung, Math. Ann. 112 (1936) , 664 - 699.

4. _____ , Über die Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung I, II , Math. Ann. 114 (1937), 1 - 28, 316 - 351 .

5. _____ , Analytische Arithmetik der positiven quadratischen Formen Dansk. Vidensk. Selsk. Math.-fys. Meddel. XVII, 12 (1940), Kobenha

6. J. Igusa, Kroneckerian model of fields of elliptic modular functions, Amer. J. Math. 81 (1959),561 - 577.

7. S. Konno, On Artin's L-functions of the algebraic curves uniformized by certain automorphic functions, J. Math. Soc. Japan, 15 (1963), 89 - 100.

8. M. Kuga, Automorphic forms and fibre varieties, Lecture notes, Chicago University, 1964, to appear.

9. S. S. Rangachari, Modulare Korrespondenzen und L-Reihen, J. Reine u. Angew. Math. 205 (1961) , 119 - 155.

10. G. Shimura, Correspondances modulaires et les fonctions $\zeta$ de courbes algébriques, J. Math. Soc. Japan 10 (1958) , 1 - 28.

11. _____ , Sur les intégrales attachées aux formes automorphes, J. Math. Soc. Japan, 11 (1959) , 291 - 311.

12. G. Shimura, On the zeta-functions of the algebraic curves uniformized by certain automorphic functions, J. Math. Soc. Japan, 13(1961), 275 - 331.

13. _____ , On Dirichlet series and abelian varieties attached to automorphic forms, Ann. Math. 76 (1962), 237 - 294.

14. G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory. Publ. Math. Soc. Japan, No. 6 , 1961.

15. T. Tamagawa, On Selberg's trace formula, J. Fac. Sci. Univ. Tokyo, Soc. I, vol. VIII, Part 2, 363 - 386.

16. _____ , On the $\zeta$-functions of a division algebra, Ann. Math. 77 (1963), 387 - 405.

17. Y. Taniyama, L-functions of number fields and zeta functions of abelian varieties, J. Math. Soc. Japan , 9 (1957) , 330 - 366.

18. A. Weil, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc. 75 (1952) , 487 - 495.

# ZETA AND L FUNCTIONS

by Jean-Pierre SERRE

The purpose of this lecture is to give the general properties of zeta functions and Artin's L functions in the setting of schemes. I will mainly restrict myself to the formal side of the theory; the connection with $\ell$-adic cohomology and Lefschetz's formula would be better discussed in a seminar.

## § 1. Zeta functions.

### 1.1. Dimension of schemes.

All schemes considered below are supposed to be of finite type over $\mathbf{Z}$.

Such a scheme $X$ has a well defined dimension, denoted by $\dim. X$. It is the maximum length $n$ of a chain

$$Z_0 \subset Z_1 \subset \ldots \subset Z_n, \qquad Z_i \neq Z_{i+1}$$

of closed irreducible subspaces of $X$. If $X$ itself is irreducible, with generic point $x$, and if $k(x)$ is the corresponding residue field, one has:

(1) $\dim. X$ = Kronecker dim. of $k(x)$.

(The Kronecker dimension of a field $E$ is the transcendence degree of $E$ over the prime field, augmented by 1 if $\mathrm{char.}\, E = 0$.)

### 1.2. Closed points.

Let $X$ be a scheme and let $x \in X$. The following properties are equivalent:

(a) $\{x\}$ is closed in $X$.

(b) The residue field $k(x)$ is finite.

The set of closed points of $X$ will be denoted by $\overline{X}$; we view it as a discrete topological space, equipped with the sheaf of fields $k(x)$; we call $\overline{X}$ the atomization of $X$. If $x \in \overline{X}$, the norm $N(x)$ of $x$ is the number of elements of $k(x)$.

1.3. Zeta functions.

The zeta function of a scheme $X$ is defined by the eulerian product

$$\zeta(X,s) = \prod_{x \in \overline{X}} \frac{1}{1 - \frac{1}{N(x)^s}} \quad . \tag{2}$$

It is easily seen that there are only a finite number of $x \in \overline{X}$ with a given norm. This is enough to show that the above product is a formal Dirichlet series $\sum_{n=1}^{\infty} a_n / n^s$, with integral coefficients. In fact, that series converges, as the following theorem shows:

THEOREM 1. The product $\zeta(X,s)$ converges absolutely for $R(s) > \dim. X$. (As usual, $R(s)$ denotes the real part of $s$.)

LEMMA. (a) Let $X$ be a finite union of schemes $X_i$. If theorem 1 is valid for each of the $X_i$'s, it is valid for $X$.

(b) If $X \to Y$ is a finite morphism, and if theorem 1 is valid for $Y$, it is valid for $X$.

Using this lemma (which is quite elementary), and induction on dimension, one reduces theorem 1 to the case $X = \operatorname{Spec} A[T_1, \ldots, T_n]$, where the ring $A$ is either $\underline{\underline{Z}}$ or $\underline{\underline{F}}_p$. In the first case, $\dim. X = n+1$, and the product (2) gives (after collecting some terms together):

$$\zeta(X,s) = \prod_p \frac{1}{1 - p^{n-s}} = \zeta(s-n) \, .$$

In the second case, $\dim. X = n$, and $\zeta(X,s) = 1/(1 - p^{n-s})$. In both cases,

we have absolute convergence for $R(s) > \dim. X$.

1.4. Analytic continuation of zeta functions.

One conjectures that $\zeta(X, s)$ can be continued as a meromorphic function in the entire $s$-plane; this, at least, has been proved for many schemes. However, in the general case, one knows only the following much weaker:

THEOREM 2. $\zeta(X, s)$ can be continued analytically (as a meromorphic function) in the half-plane $R(s) > \dim. X - \frac{1}{2}$.

The singularities of $\zeta(X, s)$ in the strip

$$\dim. X - \frac{1}{2} < R(s) \leqq \dim. X$$

are as follows:

THEOREM 3. Assume $X$ to be irreducible, and let $E$ be the residue field of its generic point.

(i) If $\text{char. } E = 0$, the only pole of $\zeta(X, s)$ in $R(s) > \dim. X - \frac{1}{2}$ is $s = \dim. X$, and it is a simple pole.

(ii) If $\text{char. } E = p \neq 0$, let $q$ be the highest power of $p$ such that $E$ contains the field $\mathbb{F}_q$. The only poles of $\zeta(X, s)$ in $R(s) > \dim. X - \frac{1}{2}$ are the points

$$s = \dim. X + \frac{2\pi i n}{\log q} \quad , \quad n \in \mathbb{Z},$$

and they are simple poles.

COROLLARY 1. For any non empty scheme $X$, the point $s = \dim. X$ is a pole of $\zeta(X, s)$. Its order is equal to the number of irreducible components of $X$ of dimension equal to $\dim. X$.

COROLLARY 2. The domain of convergence of the Dirichlet series $\zeta(X, s)$

is the half plane $R(s) > \dim. X$.

Theorem 2 and Theorem 3 are deeper than Theorem 1. Their proof uses the "Riemann hypothesis for curves" of Weil [7], combined with the technique of "fibering by curves" (i.e. maps $X \longrightarrow Y$ whose fibers are of dimension 1). One may also deduce them from the estimates of Lang - Weil [5] and Nisnevič [6].

1.5. Some properties and examples.

$\zeta(X, s)$ depends only on the atomization $\overline{X}$ of $X$. In particular, it does not change by radicial morphism, and one has

$$\zeta(X_{red}, s) = \zeta(X, s) \quad . \tag{3}$$

If $X$ is a disjoint union (which may be infinite) of subschemes $X_i$, one has:

$$\zeta(X, s) = \prod \zeta(X_i, s) \quad ,$$

with absolute convergence for $R(s) > \dim. X$. It is even enough that $\overline{X}$ be the disjoint union of the $\overline{X}_i$'s. For instance, if $f: X \longrightarrow Y$ is a morphism, one may take for $X_i$'s the fibers $X_y = f^{-1}(y)$, $y \in \overline{Y}$, and one gets:

$$\zeta(X, s) = \prod_{y \in \overline{Y}} \zeta(X_y, s). \tag{4}$$

(This -- with $Y = \mathrm{Spec}(\underline{\underline{Z}})$ -- was the original definition of Hasse - Weil.) Note that the $X_y$'s are schemes over the finite fields $k(y)$, i.e. they are "algebraic varieties".

If $X = \mathrm{Spec}(A)$, where $A$ is the ring of integers of a number field $K$, $\zeta(X, s)$ coincides with the classical zeta function $\zeta_K$ attached to $K$. For $A = \underline{\underline{Z}}$, one gets Riemann's zeta.

If $\underline{\underline{A}}^n(X)$ is the affine $n$-space over a scheme $X$, one has:

$$\zeta(\underline{\underline{A}}^n(X), s) = \zeta(X, s-n) \ .$$

Similarly:

$$\zeta(\underline{\underline{P}}^n(X), s) = \prod_{m=0}^{m=n} \zeta(X, s-m) \ .$$

1.6. Schemes over a finite field.

Let $X$ be a scheme over $\underline{\underline{F}}_q$. If $x \in \overline{X}$, the residue field $k(x)$ is a finite extension of $\underline{\underline{F}}_q$; let $\deg(x)$ be its degree. One has

$$N(x) = q^{\deg(x)},$$

and

$$(5) \qquad \zeta(X, s) = Z(X, q^{-s}),$$

where $Z(X,t)$ is the power series defined by the product:

$$(6) \qquad Z(X,t) = \prod_{x \in \overline{X}} \frac{1}{1 - t^{\deg(x)}}$$

The product (6) converges for $|t| < q^{-\dim. X}$.

THEOREM 4 (Dwork). $Z(X,t)$ is a rational function of $t$.

See [3] for the proof.

In particular, $\zeta(X,s)$ is meromorphic in the whole plane, and periodic of period $2\pi i/\log(q)$.

There is another expression of $Z(X,t)$ which is quite useful:

Let $k = \underline{\underline{F}}_q$, and denote by $k_n$ the extension of $k$ with degree $n$. Let $X_n = X(k_n)$ be the set of points of $X$ with value in $k_n/k$. Such a point $P$ can be viewed as a pair $(x,f)$, with $x \in \overline{X}$, and where $f$ is a $k$-isomorphism of $k(x)$ into $k_n$. One has:

$$\bigcup X_n = X(\overline{k}),$$

where $\overline{k}$ is the algebraic closure of $k$.

It is easily seen that the $X_n$'s are finite. If we put:

$$\nu_n = \mathrm{Card}(X_n),$$

one checks immediately that:

$$\log. Z(X,t) = \sum_{n=1}^{\infty} \nu_n t^n/n. \tag{7}$$

1.7. Frobenius.

We keep the notations of 1.6. Let $F : X \to X$ be the Frobenius morphism of $X$ into itself (i.e. $F$ is the identity on the topological space $X$, and it acts on the sheaf $O_X$ by $\varphi \mapsto \varphi^q$). If we make $F$ operate on $X(\bar{k})$, the fixed points of the $n$-th iterate $F^n$ of $F$ are the elements of $X_n$. In particular, the number $\nu_n$ is the number $A(F^n)$ of fixed points of $F^n$. This remark, first made by Weil, is the starting point of his interpretation of $\nu_n$ as a trace, in Lefschetz's style.

## § 2. L functions.

2.1. Finite groups acting on a scheme.

Let $X$ be a scheme, let $G$ be a finite group, and suppose that $G$ acts on $X$ on the right; we also assume that the quotient $X/G = Y$ exists (i.e. $X$ is a union of affine open sets which are stable by $G$). The atomization $\bar{Y}$ of $Y$ may be identified with $\bar{X}/G$. More precisely, let $x \in \bar{X}$, let $y$ be its image in $\bar{Y}$, and let $D(x)$ be the corresponding decomposition sub group; one has $g \in D(x)$ if and only if $g$ leaves $x$ fixed. There is a natural epimorphism

$$D(x) \to \mathrm{Gal}(k(x)/k(y)).$$

Its kernel $I(x)$ is called the inertia subgroup corresponding to $x$; when

$I(x) = \{1\}$, the morphism $X \to Y$ is étale at $x$.

Since $D(x)/I(x)$ can be identified with $\mathrm{Gal}(k(x)/k(y))$, it is a cyclic group, with a canonical generator $F_x$, called the Frobenius element of $x$.

2.2. Artin's definition of $L$ functions.

Let $\chi$ be a character of $G$ (i.e. a linear combination, with coefficients in $\underline{Z}$, of irreducible complex characters). For each $y \in \overline{Y}$, and for each integer $n$, let $\chi(y^n)$ be the mean value of $\chi$ on the $n$-th power $F_x^n$ of the Frobenius element $F_x \in D(x)/I(x)$, where $x \in \overline{X}$ is any lifting of $y$. Artin's definition of the $L$ function $L(X, \chi ; s)$ is the following (cf. [1]):

$$(8) \qquad \log. L(X, \chi ; s) = \sum_{y \in \overline{Y}} \sum_{n=1}^{\infty} \chi(y^n)\, N(y)^{-ns}/n.$$

When $\chi$ is the character of a linear representation $g \mapsto M(g)$, one has:

$$(9) \qquad L(X, \chi ; s) = \prod_{y \in \overline{Y}} \frac{1}{\det(1 - M(F_x)/N(y)^s)},$$

where $M(F_x)$ is again defined as the mean value of $M(g)$, for $g \mapsto F_x$.

Both expressions (8) and (9) converge absolutely when $R(s) > \dim. X$.

2.3. Formal properties of the $L$ functions.

(i) $L(X, \chi)$ depends on $X$ only through its atomization $\overline{X}$.

(ii) $L(X, \chi+\chi') = L(X, \chi).L(X, \chi')$.

(iii) If $\overline{X}$ is the disjoint union of the $\overline{X}_i$'s, with $X_i$ stable by $G$ for each $i$, one has

$$L(X, \chi ; s) = \prod L(X_i, \chi ; s),$$

with absolute convergence for $R(s) > \dim. X$.

(iv) Let $\pi : G \to G'$ be a homomorphism, and let $\pi_* X = X \times^G G'$ be the scheme deduced from $X$ by "extension of the structural group". Let $\chi'$

be a character of $G'$, and let $\pi^*\chi' = \chi' \circ \pi$ be the corresponding character of $G$. One has:

(10) $\qquad L(X, \pi^*\chi') = L(\pi_* X, \chi')$.

(v) Let $\pi : G' \to G$ be a homomorphism, and let $\pi^* X$ denote the scheme $X$ on which $G'$ operates through $\pi$. Let $\chi'$ be a character of $G'$, and let $\pi_*\chi'$ be its direct image, which is a character of $G$ (when $G'$ is a subgroup of $G$, $\pi_*\chi'$ is the "induced character" of $\chi'$). One has:

(11) $\qquad L(X, \pi_*\chi') = L(\pi^* X, \chi')$.

(vi) Let $X = \mathrm{Spec}(\underline{\underline{F}}_{q^n})$, $Y = \mathrm{Spec}(\underline{\underline{F}}_q)$, $G = \mathrm{Gal}(\underline{\underline{F}}_{q^n}/\underline{\underline{F}}_q)$, and $\chi$ an irreducible character of $G$. One has:

(12) $\qquad L(X, \chi : s) = \dfrac{1}{1 - \chi(F)\, q^{-s}}$ ,

where $F$ is the Frobenius element of $G$.

It is not hard to see that properties (i) to (vi) characterize uniquely the $L$ functions.

(vii) If $\chi = 1$ (unit character), $L(X, 1) = \zeta(X/G)$.

(viii) If $\chi = r$ (character of the regular representation), one has:

$$L(X, r) = \zeta(X).$$

Combining (viii) and (ii), one gets the following formula (which is one of the main reasons for introducing $L$ functions):

(13) $\qquad \zeta(X) = \prod_{\chi \in \mathrm{Irr}(G)} L(X, \chi)^{\deg(\chi)}$,

where $\mathrm{Irr}(G)$ denotes the set of irreducible characters of $G$, and $\deg(\chi) = \chi(1)$.

There is an analogous result for $\zeta(X/H)$, when $H$ is a subgroup of $G$; one just replaces the regular representation by the permutation representation of $G/H$.

2.4. Schemes over a finite field.

Let $X$ be an $\underline{\underline{F}}_q$ - scheme, and assume that the operations of $G$ are $\underline{\underline{F}}_q$ - automorphisms of $X$. The scheme $Y = X/G$ is then also an $\underline{\underline{F}}_q$ - scheme.

On the set $X(\bar{k})$, we have two kinds of operators: the Frobenius endomorphism $F$ (cf. n° 1.7) and the automorphisms defined by the elements of $G$; if $g \in G$, one has $F \circ g = g \circ F$.

If we put as usual $t = q^{-s}$, we can transform $L(X, \chi; s)$ into a function $\underline{L}(X, \chi; t)$ of $t$. An elementary calculation gives:

$$(14) \qquad \log. \underline{L}(X, \chi; t) = \sum_{n=1}^{\infty} \nu_n(\chi)\, t^n/n,$$

with:

$$(15) \qquad \nu_n(\chi) = \frac{1}{(G)} \sum_{g \in G} \chi(g^{-1})\, \Lambda(gF^n),$$

where $(G) = \mathrm{Card}(G)$, and $\Lambda(gF^n)$ is the number of fixed points of $gF^n$ (acting on $X(\bar{k})$).

(These formulae could have been used to define the $L$ functions; they make the verification of properties (i) to (vi) very easy.)

Remark. It is not yet known that $\underline{L}(X, \chi; t)$ is a rational function of $t$. However, this is true in the following special cases:

(a) When $X$ is projective and smooth over $\underline{\underline{F}}_q$: this follows from $\ell$-adic cohomology (Artin - Grothendieck).

(b) When Artin - Schreier or Kummer theory applies, i.e. when $G$ is cyclic of order $p^N$, or of order $m$ prime to $p$, with $m$ dividing $q - 1$. This can be proved by Dwork's method; the case $G = \underline{\underline{Z}}/p\underline{\underline{Z}}$ has been studied in some detail by Bombieri.

2.5. Artin - Schreier extensions.

It would be easy -- but too long -- to give various examples of $L$ functions, in particular for an abelian group $G$. I will limit myself to one such example:

Let $Y$ be an $\underline{\underline{F}}_q$ - scheme, and let $a$ be a section of the sheaf $\underline{\underline{O}}_Y$. In the affine line $Y[T]$, let $X$ be the closed subscheme defined by the equation

$$T^p - T = a.$$

If we put $G = \underline{\underline{Z}}/p\underline{\underline{Z}}$, the group $G$ acts on $X$ by $T \mapsto T + 1$, and $X/G = Y$; we get in this way an étale covering. Let $w$ be a $p$-th root of unity in $\underline{\underline{C}}$, and let $\chi$ be the character of $G$ defined by $\chi(n) = w^n$. The $L$ function $\underline{\underline{L}}(X, \chi ; t)$ is given by formula (14); its coefficients $\nu_n(\chi)$ can be written here in the following form:

$$(16) \qquad \nu_n(\chi) = \sum_{y \in Y_n} w^{Tr_n a(y)},$$

where $Y_n = Y(k_n)$, and $Tr_n$ is the trace map from $k_n = \underline{\underline{F}}_{q^n}$ to $\underline{\underline{F}}_p$. The above expression is a typical "exponential sum". If, for instance, we take for $Y$ the multiplicative group $\underline{\underline{G}}_m$, and put $a = \lambda y + \mu y^{-1}$, we get the so-called Kloosterman sums. This connection between $L$ functions and exponential sums was first noticed by Davenport - Hasse [2], and then used by Weil [8] to give estimates in the 1-dimensional case.

2.6. Analytic continuation of $L$ functions.

Theorems 2 and 3 have analogues for $L$ functions. First:

THEOREM 5. $L(X, \chi ; s)$ can be continued analytically (as a meromorphic function) in the half - plane $R(s) > \dim. X - \frac{1}{2}$.

The singularities of $L(X,\chi;s)$ in the critical strip

$$\dim.X - \tfrac{1}{2} < R(s) \leq \dim.X$$

can be determined, or rather reduced to the classical case $\dim.X = 1$. One uses the following variant of the "fibering by curves" method:

LEMMA. Let $f: X \to X'$ be a morphism which commutes with the action of the group $G$. Assume that all geometric fibers of $f$ are irreducible curves. Then:

$$(17) \qquad L(X,\chi;s) = H(s).L(X',\chi;s-1)\ ,$$

where $H(s)$ is holomorphic and $\neq 0$ for $R(s) > \dim.X - \frac{1}{2}$.

This lemma gives a reduction process to dimension 1 (and even to dimension 0 if $X$ is a scheme over a finite field). The result obtained in this way is a bit involved, and I will just state a special case:

THEOREM 6. Assume that $X$ is irreducible, and that $G$ operates faithfully on the residue field $E$ of the generic point of $X$. Let $\chi$ be a character of $G$, and let $\langle \chi, 1\rangle$ be the multiplicity of the identity character $1$ in $\chi$. The order of $L(X,\chi)$ at $s = \dim.X$ is equal to $-\langle \chi, 1\rangle$.

COROLLARY. If $\chi$ is a non trivial irreducible character, $L(X,\chi)$ is holomorphic and $\neq 0$ at the point $s = \dim.X$.

2.7. Artin - Čebotarev's density theorem.

Let $Y$ be an irreducible scheme of dimension $n \geq 1$. Using the fact that $\zeta(Y,s)$ has a simple pole at $s = n$, one gets easily:

$$(18) \qquad \sum_{y \in \overline{Y}} \frac{1}{N(y)^s} \sim \log \frac{1}{s-n} \qquad \text{for } s \to n.$$

A subset $M$ of $\overline{Y}$ has a Dirichlet density $m$ if one has:

$$(19) \qquad \Big(\sum_{y \in M} \frac{1}{N(y)^s}\Big) \Big/ \log \frac{1}{s-n} \to m \quad \text{for } s \to n.$$

(For $Y = \mathrm{Spec}(\underline{\underline{Z}})$, this is the usual definition of the Dirichlet density of a set of prime numbers.)

Now let $X$ verify the assumptions of Theorem 6, and let $Y = X/G$. Assume that $\dim. X \geq 1$, and that $G$ operates freely (i.e. $I(x) = \{1\}$ for all $x \in \overline{X}$). If $y \in \overline{Y}$, the Frobenius element $F_x$ of a corresponding point $x \in \overline{X}$ is a well defined element of $G$, and its conjugation class $\{F_x\} = F_y$ depends only on $y$.

THEOREM 7. Let $R \subset G$ be a subset of $G$ stable by conjugation. The set $\overline{Y}_R$ of elements $y \in \overline{Y}$ such that $F_y \subset R$ has Dirichlet density $\mathrm{Card}(R)/\mathrm{Card}(G)$.

This follows by standard arguments from the corollary to Theorem 6.

COROLLARY. $\overline{Y}_R$ is infinite if $R \neq \emptyset$.

Remark. A slightly more precise result has been obtained by Lang [4] for "geometric" coverings, and also for coverings obtained by extension of the ground field.

# BIBLIOGRAPHY


[1] E. Artin. Zur Theorie der L - Reihen mit allgemeinen Gruppencharakteren. Abh. Hamb., 8, 1930.

[2] H. Davenport and H. Hasse. Die Nullstellen der Kongruenzzetafunktionen im gewissen zyklischen Fällen. Crelle Journ., 172, 1935, p. 151-182.

[3] B. Dwork. On the rationality of the zeta function of an algebraic variety. Amer. Journ. of Math., 82, 1960, p. 631-648.

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

[5] S. Lang and A. Weil. Number of points of varieties in finite fields. Amer. Journ. of Math., 76, 1954, p. 819-827.

[6] L. Nisnevič. Number of points of algebraic varieties over finite fields [in Russian]. Dokl. Akad. Nauk, 99, 1954, p. 17-20.

[7] A. Weil. Sur les courbes algébriques et les variétés qui s'en déduisent. Act. Sci. Ind. n° 1041, Paris, Hermann, 1948.

[8] A. Weil. On some exponential sums. Proc. Nat. Acad. Sci. USA, 34, 1948, p. 204-207.

[9] A. Weil. Number of solutions of equations in finite fields. Bull. Amer. Math. Soc., 55, 1949, p. 497-508.