I

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

The following is a list of the participants who will be attending the Institute.

ABHYANKAR, Shreeram
Harvard University

ADELBERG, Arnold
Grinnell College

ANDREOTTI, Aldo
Brandeis University

ARTIN, Michael
Massachusetts Institute of Technology

ATIYAH, Michael F.
Oxford University

AUSLANDER, Maurice
Brandeis University

BARSOTTI, Iacopo
Universita di Pisa

BASS, Hyman
Columbia University

BOMBIERI, Enrico
Milano, Italy

BOTT, Raoul
Harvard University

BUCHSBAUM, David A.
Brandeis University

CASSELS, J. W. S.
Trinity College

CHOW, Wei Liang
Johns Hopkins University

de AZEVEDO, Alberto
Harvard University

DWORK, Bernard M.
Johns Hopkins University

EHRENPREIS, Leon
New York University

FOGARTY, John
Harvard University

FULTON, William E.
Princeton University

GERSTENHABER, Murray
University of Pennsylvania

GREENBERG, Marvin J.
University of California, Berkeley

GREENLEAF, Newcomb
Harvard University

GRIFFITHS, Phillip A.
University of California, Berkeley

GUNNING, Robert C.
Princeton University

HARTSHORNE, Robert C.
Harvard University

HIRONAKA, Heisuke
Brandeis University

HOYT, William
Brandeis University

IGUSA, Jun-Ichi
Johns Hopkins University

IRELAND, Kenneth
Brandeis University

KATZ, Nicholas M.
Johns Hopkins University

KIM, Ki
Brandeis University

KLEIMAN, Stephen
Harvard University

KODAIRA, Kunihiko
Johns Hopkins University

KOHN, Joseph J.
Brandeis University

KUGA, Michio
Institute for Advanced Study

KURANISHI, Masatake
Columbia University

LANG, Serge
Columbia University

LICHTENBAUM, Stephen
Harvard University

LIPMAN, Joseph
Harvard University

LLUIS, Emilio R.
Ciudad Universitaria

LUBIN, Jonathan D.
Bowdoin College

MATSUSAKA, Teruhisa
Brandeis University

MATTUCK, Arthur P.
Massachusetts Institute of Technology

MAYER, Alan
Brandeis University

MONSKY, Paul
Princeton University

MUMFORD, David B.
Harvard University

MURRE, J. P.
Voorschoten, Netherlands

NAGATA, Masayoshi
Kyoto University

NAKAI, Yoshikazu
Brandeis University

NASH, John
Institute for Advanced Study

ODA, Tadeo
Nagoya University

OGG, Andrew
University of California, Berkeley

OHM, Jack E.
University of Wisconsin

ONA, Takashi
University of Pennsylvania

PENDLETON, Robert
Dartmouth College

QUILLEN, Daniel
Harvard University

RAUCH, Harry E.
Yeshiva University

RECILLAS, Felix J.
Ciudad Universitaria

RIM, Dock S.
Brandeis University

ROSENLICHT, Maxwell A.
University of California, Berkeley

ROSSI, Hugo
Brandeis University

SAMUEL, Pierre
University of Paris

SATAKE, Ichiro
University of Chicago

SATO, Mikio
Columbia University

SCHLESSINGER, J. Michael
Harvard University

SEIDENBERG, Abraham
Harvard University

SEN, Shankar
Harvard University

SERRE, Jean-Pierre
College of France

SHATZ, Stephen
Stanford University

SHIMURA, Goro
Princeton University

SPENCER, Donald C.
Stanford University

TATE, John T.
Harvard University

VERDIER, Jean-Louis
Bagneaux (Seine), France

VESENTINI, Edoardo
Harvard University

WASHNITZER, Gerard
Princeton University

ZARISKI, Oscar
Harvard University

GLW:mll
6-10-64

REVISED PROGRAM OF THE SUMMER INSTITUTE IN ALGEBRAIC GEOMETRY

(July 6 - July 31, 1964)

Monday, July 6: REGISTRATION DAY.

I. THEORY OF SINGULARITIES.

Tuesday, July 7:

10:00 - 11:00 a.m.	S. Abhyankar. Current status of the resolution problem.
11:30 - 12:30 p.m.	H. Hironaka. Equivalences and deformations of isolated singularities.
4:30 - 5:30 p.m.	O. Zariski. Equisingularity and related questions of classification of singularities.

II. CLASSIFICATION OF SURFACES AND MODULI.

Wednesday, July 8:

10:00 - 11:00 a.m.	K. Kodaira. On the structure of compact complex analytic surfaces.
11:30 - 12:30 p.m.	T. Matsusaka. Deformations and varieties of moduli.
4:30 - 5:30 p.m.	D. Mumford. The boundary points of moduli schemes.

Thursday, July 9:

10:00 - 11:00 a.m.	M. Nagata. Invariants of a group in an affine ring.
11:30 - 12:30 p.m.	M. Rosenlicht. Transformation spaces, quotient spaces, and some classification problem.

Wednesday, July 15:

4:30 - 5:30 p.m.	J. Igusa. On the Siegel modular variety.

III. GROTHENDIECK COHOMOLOGY.

Friday, July 10:

10:00 - 11:00 a.m.	M. Artin. Etale cohomology of schemes.

11:30 - 12:30 p.m.	<u>J. L. Verdier</u>. A duality theorem in the etale cohomology of schemes.
4:30 - 5:30 p.m.	<u>J. Tate</u>. Etale cohomology over number fields.

IV. ZETA FUNCTIONS AND ARITHMETIC OF ABELIAN VARIETIES.

Monday, July 13:

10:00 - 11:00 a.m.	<u>J. W. S. Cassels</u>. The arithmetic of elliptic curves and abelian varieties.
11:30 - 12:30 p.m.	<u>B. M. Dwork</u>. (Title not available)
4:30 - 5:30 p.m.	<u>B. Shimura</u>. The Zeta-function of an algebraic variety and automorphic functions.

Tuesday, July 14:

4:30 - 5:30 p.m.	<u>J. P. Serre</u>. L-Series of schemes.

Oscar Zariski, Chairman
Organizing Committee

TABLE OF CONTENTS

CURRENT STATUS OF THE RESOLUTION PROBLEM

by

Shreeram S. Abhyankar

§1. The problem and its history.

The problem can be stated thus:

Resolution Problem. Given a function field K over a pseudogeometric Dedekind domain k does there exist a nonsingular projective model of K over k ?

Before giving the history of the problem let us recall the definitions of the terms used above.

DEFINITION. By a Dedekind domain we mean a normal (i.e., integrally closed in its quotient field) noetherian (integral) domain in which every nonzero prime ideal is maximal; note that then any field is a Dedekind domain. A ring (commutative with identity) k is said to be pseudogeometric if k is noetherian and for every prime ideal P in k we have that the integral closure of k/P in any finite algebraic extension of the quotient field of k/P is a finite (k/P)-module. Note that: every field is pseudogeometric; every Dedekind domain of characteristic zero is pseudogeometric; a Dedekind domain k is pseudogeometric if and only if the integral closure of k in any finite algebraic extension of the quotient field of k is a finite k-module.

By an affine ring over a domain k we mean an overdomain of k which is a finitely generated ring extension of k. A local ring (i.e., a noetherian ring with a unique maximal ideal) R is said to be a spot over a domain k if R is the quotient ring A_P of an affine ring A over k with respect to a prime ideal P in A. The significance of the notion of pseudogeometric is the theorem of Nagata to the effect that if k is a pseudogeometric domain then every affine ring over k is pseudogeometric and so is every spot over k. By a function field over a domain k we mean a field K which is a spot over k, i.e., K is the quotient field of an affine ring over k. Given a function field K over a domain k, by a projective model of K over k we mean a nonempty set V of local domains with quotient field K such that there exists a finite number of nonzero elements $x_0, \ldots, x_m$ in K such that $V = \bigcup_{i=0}^{m} V_i$ where V_i is the set of all quotient rings of $k[x_0/x_i, \ldots, x_m/x_i]$ with respect to the various prime ideals in $k[x_0/x_i, \ldots, x_m/x_i]$; V is said to be nonsingular if every element in V is regular.

<u>History.</u> Let K be a function field over a pseudogeometric Dedekind domain k, let n' be the transcendence degree of K over the quotient field of k, and let n be the absolute dimension of K over k, i.e., n = n' if k is a field, and n = 1 + n' if k is not a field. The Resolution Problem has been settled affirmatively in the following cases: For n = 1 the solution is classical. For n = 2 and k = the field of complex numbers, after several possible solutions by the Italians (notably by Alabanese and Levi)

the first rigorous solution was given by Walker in 1935; Walker's solution makes use of the local solution (i.e., solution of the local uniformization problem which is the localized version of the Resolution Problem) for $n = 2$ and $k =$ the field of complex numbers given by Jung in 1908 in the Crelle Journal. When k is a field of characteristic zero, Zariski gave a solution for $n = 2$ in 1939 - 1942 and for $n = 3$ in 1944; in 1940 Zariski also gave a local solution for n arbitrary and $k =$ a field of characteristic zero. For $n = 2$ and $k =$ a perfect field, Abhyankar gave a solution in 1956. Finally, in 1964 Hironaka gave a solution for n arbitrary and $k =$ a field of characteristic zero. All these are publication dates and all the solutions beginning with Walker's appeared in the Annals of Mathematics. For $n = 2$, a rigorous version of Albanese's proof was given by Artin in the spring of 1963 which works when k is an algebraically closed field of characteristic different from 2. In November 1963 I gave a solution when $n = 2$ and k/P is perfect for every maximal ideal P in k; this proof of the Arithmetical Case is being published. In the last few months I have obtained a solution for $n = 3$ and $k =$ an algebraically closed field (of any characteristic); to be on the safe side here I should say that this is a possible solution in the sense that I have proved several pieces and I roughly see how to put them together but as yet I did not have the time to write up these peices systematically and to fit them together. In any case my present investigations have just begun and they would take a year or more to run their full course. So actually I would have been happier to give today's talk after a year or so because then I could have simply said that this is what I can prove and this is what I cannot. Presently I can only say what is cooking. The reason why after a lapse of some eight years I have come back to the resolution problem is twofold. The primary reason was that the fall of 1963 was the first time after 1955 when I got an opportunity to be in Zariski's neighbourhood(not a Zariski neighbourhood); it is a theorem that to resolve singularities it is necessary to be near Zariski; the resolution problem consists of proving the sufficiency of this condition. The secondary reason was that after Hironaka's outstanding work in characteristic zero, I heard a story from several people to the effect: "We have heard that you are planning to take over the work on the problem where Hironaka has left it off". Although I was definitely not the source of this rumour, nevertheless it prompted me to work.

§2. Embedded resolution

Today I shall say nothing about the arithmetical case. Henceforth all varieties will be defined over an algebraically closed ground field of characteristic p which may or may not be zero. Having once stated the problem precisely, henceforth I shall speak quite informally. A common feature of all the above cited proofs is that to prove resolution for dimension n one needs a stronger result for dimension less than n which includes at least the following:

Embedded Resolution. Given a nonsingular projective algebraic variety W of dimension n and given a hypersurface H in W, there exists a composite monoidal transformation $q : W' \longrightarrow W$ such that the total transform $q^{-1}(H)$ of H has only normal crossings.

Concerning the definitions of the terms used above I shall say only this: Given any irreducible subvariety D of an irreducible algebraic variety W there exists a well defined birational map $q : W' \longrightarrow W$ called the monoidal transformation of W with center D; q is biregular on $W - D$; if W and D are nonsingular then so is W'; if D is a point then q is called the quadratic transformation with center D. If $q_1 : W_1 \longrightarrow W$, $q_2 : W_2 \longrightarrow W_1, \ldots, q_t : W_t \longrightarrow W_{t-1}$ is a sequence of monoidal transformations with nonsingular centers then the resulting birational map $q: W_t \longrightarrow W$ is called a composite monoidal transformation. Henceforth all monoidal transformations will be assumed to have nonsingular centers. A hypersurface H in a nonsingular variety W is said to have only normal crossings if for every point P of W there exist regular parameters $x_1, \ldots, x_n$ on W at P such that H is defined by $x_1 \ldots x_m = 0$ at P for some $m \leqq n$.

Usually, after Embedded Resolution for n and before Resolution for n one proves the following:

Dominance (or removal of points of indeterminacy). Given two nonsingular projective models W and W^* of an n dimensional function field, there exists a composite monoidal transformation $W' \longrightarrow W$ such that W' dominates W^*.

Concerning Embedded Resolution I can definitely say that I have a proof for $n = 3$ in any characteristic; and this is the major step in the possible proof of Resolution for $n = 3$ which I spoke of. Another dividend of this result is that I believe one can now prove the birational invariance of the arithmetic genus for dimension 3. In my proof of Embedded Resolution for $n = 3$ I draw heavily from Zariski's proof of the same result in characteristic zero which he gave in 1944 and also from the simplified proof of this which Zariski gave in a note in 1962 in the Rendiconti... Lincei.

§3. Peculiarities of nonzero characteristic

I shall now make various comments as to how the case $p \neq 0$ differs from the case $p = 0$ and what are the possible ways to make up for this difference. Let me say explicitly that it is not my purpose to find a proof which will be essentially new for $p = 0$. I am only trying to develop an algorithm or a calculus in $p \neq 0$ which will enable us to modify any given proof (of resolution) for $p = 0$ so that it will work also for $p \neq 0$.

(1) Binomial theorem. Algebraically speaking, the basic reason why the $p = 0$ proofs (of Zariski and Hironaka) fail for $p \neq 0$ is this:

Let

$$(Z + Y)^m = Z^m + a_1 Z^{m-1}Y + a_2 Z^{m-2}Y^2 + \ldots + Y^m .$$

Then $a_1 \neq 0$ if $m \not\equiv 0(p)$, and $a_1 = 0$ if $m \equiv 0(p)$. More generally let

$$f(Z) = Z^m + f_1 Z^{m-1} + \ldots + f_m$$

and

$$g(Z) = f(Z + Y) = Z^m + g_1 Z^{m-1} + \ldots + g_m .$$

Then what is the relationship between the f_i and the g_j, i.e., which of the f_i affect a particular g_j and how much?

(2) <u>An example of</u> (1). Let

$$V : G(Z_1, \ldots, Z_{n+1}) = 0$$

be an algebroid hypersurface in the $n + 1$ dimensional local space A_{n+1}. Let m be the multiplicity of V. Then upon making a linear transformation and invoking the Weierstrass Preparation Theorem we get

$$V : Z^m + g_1(Y_1, \ldots, Y_n)Z^{m-1} + \ldots + g_m(Y_1, \ldots, Y_n) = 0$$

where $g_i(0, \ldots, 0) = 0$. Let g be the product of those g_i which are non-zero. Let

$$H : g(Y_1, \ldots, Y_n) = 0 .$$

Then H is an hypersurface in the n dimensional local space A_n. Apply Embedded Resolution to get a composite monoidal transformation $q : B \longrightarrow A_n$ such that $q^{-1}(H)$ has only normal crossings. Let $X_1, \ldots, X_n$ be suitable parameters at a point P in B. This amounts to substituting certain power series $u_1(X_1, \ldots, X_n), \ldots, u_n(X_1, \ldots, X_n)$ for $Y_1, \ldots, Y_n$ in $g(Y_1, \ldots, Y_n)$ so that

$$g(u_1(X_1, \ldots, X_n), \ldots, u_n(X_1, \ldots, X_n)) = g'(X_1, \ldots, X_n) X_1^{a(1)} \ldots X_n^{a(n)}$$

where $g'(0, \ldots, 0) \neq 0$ and $a(1), \ldots, a(n)$ are nonnegative integers. Then actually

$$g_i(u_1(X_1, \ldots, X_n), \ldots, u_n(X_1, \ldots, X_n)) = g_i'(X_1, \ldots, X_n) X_1^{a(i,1)} \ldots X_n^{a(i,n)}$$

for all i for which $g_i \neq 0$, where $g_i'(0, \ldots, 0) \neq 0$ and $a(i,j)$ are nonnegative integers. q induces $q^* : B \times A_1 \longrightarrow A_{n+1}$. Let V^* be the proper transform of V by q^{*-1}. Then at the point $(P, 0)$, V^* is given by

$$V^* : Z^m + \sum_{0 < i \leqq m,\, g_i \neq 0} g_i'(X_1, \ldots, X_n) X_1^{a(i,1)} \ldots X_n^{a(i,n)} Z^{m-i} = 0$$

For the sake of simplicity let us suppose that $a(i,j) = 0$ whenever $j \neq 1$. Let b be the greatest integer such that $b \leqq a(i,1)/i$ for all i for which $g_i \neq 0$. Then $a(i',1) - bi' < i'$ for some i'. Make the composite monoidal transformation given by : $Z = Z^* X_1^b$. Let V' be the proper transform of V^* under this transformation. Let Q be a point of V'. Then there exists a unique element d in k such that "$Z^* = d$ at Q" Let $Z' = Z^* - d$. Then $X_1, \ldots, X_n$, Z' are parameters at Q and at Q we have

$$V' : f(X_1, \ldots, X_n, Z') = 0$$

where

$$f(X_1, \ldots, X_n, Z')$$

$$= (Z' + d)^m + \sum_{0<i\leq m,\ g_i\neq 0} g_i'(X_1, \ldots, X_n) X_1^{a(i,1)-bi} (Z' + d)^{m-i} \ .$$

Let m' be the multiplicity of V' at Q. Since $a(i',1) - bi' < i'$ for some i', we get that if $d = 0$ then $m' < m$; a reduction! So now suppose that $d \neq 0$. At this point there are various essentially equivalent ways of arguing provided $m \not\equiv 0(p)$. For instance, following Hironaka, we can make the initial coordinate transformation $Z \longrightarrow Z - (1/m)g_1$ which will have the effect that the coefficient of Z^{m-1} will be zero, i.e., we will then have $g_1 = 0$ and hence

$f(X_1, \ldots, X_n, Z') = Z'^m + dmZ'^{m-1} +$ terms of degree less than $m-1$ in Z'.

Then $m' < m$ because $dm \neq 0$. However if $m \equiv 0(p)$ then in the first place we cannot make the transformation $Z \longrightarrow (1/m)g_1$, and in the second place even if g_1 was zero to begin with we still cannot conclude that $m' < m$

because now $dm = 0$. We shall now make several observations.

(3). Peculiarity arises when the multiplicity is divisible by p.

(4) The most primitive case of the above peculiarity is afforded by: $Z^p - g(Y_1, \ldots, Y_n) = 0$. The two dimension case (i.e., $n = 2$) of this was explicitly mentioned by Zariski in his 1950 address and there he pronounced it "intractable".

(5) It is not necessary to kill g_1 completely, i.e., it is enough to kill the terms of low degree in g_1. Because then $a(1,1) > b$ and hence again the coefficient of Z'^{m-1} in $f(Z')$ will be a unit. In any case if we have $a(1,1) > b$ then we are all right. In other words, the X_1-value of g_1 should be big enough compared to the X_1-values of the other g_i. If $m \equiv 0(p)$ then of course g_1 does not play the dominant role. But it turns out that even then we would be in a reasonable shape if say

$$(X_1\text{-value of } g_i) \geqq (i/m)(X_1\text{-value of } g_m) \text{ for } i = 1, \ldots, m.$$

It can be shown that if the above inequality fails for some i then X_1 must split in the covering $V' \longrightarrow$ (space of $X_1, \ldots, X_n$), i.e., X_1 must split in the field extension given by $f(X_1, \ldots, X_n, Z')$. So one should try to arrange that X_1 does not split.

(6). In the general case, i.e., when one does not assume $a(i,j) = 0$ for $j \neq 1$, one tries to arrange matters so that for any $i \neq i^*$ either g_i divides g_{i*} or g_{i*} divides g_i, i.e., either $a(i,j) \leqq a(i^*,j)$ for all j or $a(i^*, j) \leqq a(i, j)$ for all j. This really means that instead of only applying "Embedded Resolution" we also invoke "Dominance". In this general case one should accordingly try to arrange that each of the X_j which occur with a positive exponent does not split in the field extension given by f.

(7) Instead of killing g_1, Zariski used differentiation arguments. But then after all the binomial theorem and differentiation are in essence one and the same thing.

In §4 and §5 I shall further elucidate observations (5) and (4) respectively.

§4. Nonsplitting

Let W be a nonsingular projective algebraic variety of dimension n and let V be the normalization of W in a finite algebraic separable extension of the function field of W, i.e., we have a covering map $V \longrightarrow W$. Let D be the branch locus on W. By Embedded Resolution we can find a composite monoidal transformation $q: W' \longrightarrow W$ such that $q^{-1}(D)$ has only normal crossings. Let $h: V' \longrightarrow W'$ be the corresponding covering map and let D' be the branch locus on W'. Then $D' \subset q^{-1}(D)$. It can then be shown if $p = 0$ (or more generally if $V' \longrightarrow W'$ is a tame covering) then the irreducible components of $q^{-1}(D)$ do not split locally on

V', i.e., if $P' \in V'$ lies above $Q' \in W'$ and E is any irreducible component of $q^{-1}(D)$ at Q' then only one locally irreducible component of $h^{-1}(E)$ passes through P'. In other words, if $f(Z) = Z^m + g_1 Z^{m-1} + \dots + g_m$ is a local equation of the covering $P' \longrightarrow Q'$ and $X_1, \dots, X_n$ are parameters at Q' such that $q^{-1}(D) \subset (X_1 \cdots X_n = 0)$ then for $i = 1, \dots, n$ we have that the valuation at Q' given by X_i does not split in the field extension given by $f(Z)$. Thus what was achieved by Hironaka by killing g_1 and by Zariski by using differentiation arguments can also be achieved by simplifying the branch locus. The idea of simplifying the branch locus to resolve the singularities of V was actually used by Jung for $n = 2$ and $k =$ the field of complex numbers, and it was also proposed by Zariski (1954: Bulletin des Sciences Mathematiques) as a possible method of resolutinn of singularities for all n when $p = 0$; also Zariski used this idea in his Lincei note cited in §2. Both of them used this only to have a nice structure for the local ring of P' and not for the nonsplitting business. However, we thus see that this Jungian method of simplifying the branch locus (i.e., transforming the discriminant into a monomial times a unit) and the Zariski-Hironaka method of transforming the coefficients into monomials times units are in essence very closely related, although they may not appear so at first sight.

Actually in 1953, Zariski had suggested to me to study Jung's method and to see whether it could be used for resolution of singularities of a surface in $p \neq 0$. At that time I ended up by showing that in $p \neq 0$: the local Galois group above a simple point of the branch locus can be unsolvable, and a point lying above a simple point of the branch locus can be singular, and hence Jung's method cannot be used. The examples were published in 1955 in the American Journal where it was shown that they can occur only for nontame coverings. There I also showed that although the nonsplitting holds for tame coverings, in general it does not, and I went on to comment that: this "local splitting of a simple branch variety by itself" is the real reason behind the peculiarity in $p \neq 0$. Later on in a 1957 paper in the American Journal I exploited a similar splitting of a branch point on a curve to get results like the following: every curve in $p \neq 0$ can be projected onto the projective line so as to have only one branch point. On the other hand, in a series of papers published in the American Journal in 1959-1960 I used the nonsplitting for tame coverings to study the tame fundamental group of an algebraic variety.

Now after eight years the circle is completed. Namely, it turned out that (for a covering of a surface where the covering degree is either not divisible by p or is a power of p) if we keep applying quadratic transformations, even after the stage when the branch locus has only normal crossings, then eventually we shall reach a stage when we have nonsplitting; and what is more important is that we can reach a stage which is stable, i.e., when the nonsplitting is not destroyed by applying more quadratic transformations; needless to remark that the number of quadratic transformations required to achieve such a stable nonsplitting stage depends on the given covering. Moreover, in the end we reach a Jungian situation after all. This realization was forced upon me by working on the arithmetical case in which no single method seems to work by itself. The arriving at a stable nonsplitting stage is also the main novel aspect of my proof of Embedded Resolution for $n = 3$, i.e., for surfaces.

All this leads me to pose the following conjectural supplement to Embedded Resolution.

Supplement 1. Let W be a nonsingular projective algebraic variety of dimension n, let V be the normalization of W in a finite algebraic separable extension of the function field of W, and let D be the branch locus on W for the covering $V \longrightarrow W$. You may assume that D has only normal crossings. Find a composite monoidal transformation $q : W' \longrightarrow W$ such that nonsplitting holds for $q^{-1}(D)$ relative to the corresponding covering $V' \longrightarrow W'$. Do this in some stable sense.

It is proposed to use this as an inductive step in the general resolution problem.

§5. Units cannot be neglected

Let us now consider the primitive case

$$V : Z^p - g(Y_1, \ldots, Y_n) = 0 .$$

The nonsplitting business clearly has no bearing on this. By Embedded Resolution we can achieve

$$g(Y_1, \ldots, Y_n) = g'(X_1, \ldots, X_n) X_1^{a(1)} \ldots X_n^{a(n)}$$

where $g'(0, \ldots, 0) \neq 0$. If at least one of the $a(i)$ is not divisible by p then we can do something. But if $a(i) \equiv 0(p)$ for all i then upon making a composite monoidal transformation we get

$$V' : Z'^p - g^*(X_1, \ldots, X_n) = 0$$

where

$$g^*(X_1, \ldots, X_n) = g'(X_1, \ldots, X_n) - g'(0, \ldots, 0).$$

So we achieved nothing because the order of $g^*(X_1, \ldots, X_n)$ may even be greater than the order of $g(Y_1, \ldots, Y_n)$. In other words, in $p \neq 0$ we cannot neglect the unit $g'(X_1, \ldots, X_n)$. A similar situation prevails for

$$V : Z^{p^u} - g(Y_1, \ldots, Y_n) = 0 .$$

Thus we are led to another conjectural supplement to Embedded Resolution; this one cannot be formulated completely geometrically, i.e., we cannot talk of a hypersurface but we must actually deal with a power series, because we are now not interested in a principal ideal but in a specific power series.

<u>Supplement</u> 2. Let $m = p^u$ where u is a positive integer. Let g be an element in the power series ring $k[[Y_1, \ldots, Y_n]]$ such that $g \notin k[[Y_1^m, \ldots, Y_n^m]]$. Find a composite monoidal transformation $q : B \longrightarrow A_n$, where A_n is the local space of $Y_1, \ldots, Y_n$, such that at any $P \in B$ there exist suitable parameters $X_1, \ldots, X_n$ such that upon considering g as an element in $k[[X_1, \ldots, X_n]]$ we have that

$$g = h^m + (X_1^{a(1)} \ldots X_n^{a(n)})^m g'$$

where $a(1), \ldots, a(n)$ are nonnegative integers and h and g' are elements in $k[[X_1, \ldots, X_n]]$ such that $0 <$ (order of g') $< m$.

Actually this is not entirely satisfactory because it is not a stable situation. One must ask for a stable situation. Here I shall not pursue this matter further because things would get too technical.

As such the primitive case may not occur in practice because we can choose a separating transcendence basis, etc. However, in the separable case

$$Z^p + g_1(Y_1,\ldots,Y_n)Z^{p-1} + \ldots + g_p(Y_1,\ldots,Y_n)$$

the nonsplitting business will help only to see to it that $g_1,\ldots,g_{p-1}$ do not intefere too much. The game is still to be played with g_p. In other words, it is proposed that:

(general case) = (primitive case) + (nonsplitting) .

Anyway, this is how I carry out things for surfaces.

§6. Resolution for coverings

I shall conclude by mentioning a more general resolution problem which is of interest in itself and some form of which may very well be useful in an inductive set up for the original resolution problem

(1). Give an intrinsic definition of a Jungian local domain, i.e., of a normal local domain which in case of characteristic zero can be projected onto a regular local domain so that the branch locus has a normal crossing; (for dimension 2 I have done this in a forthcoming paper).

(2). Given a function field K and a finite algebraic separable extension L of K, does there exist a nonsingular model of K whose normalization in L is Jungian?

(3). Given a function field K and a finite algebraic separable extension L of K, does there exist a Jungian model of K whose normalization in L is nonsingular?

I shall only remark that (3) is nontrivial even when the characteristic is zero and we require the model of K to be only normal.

EQUIVALENCES AND DEFORMATIONS OF ISOLATED SINGULARITIES

by H. Hironaka

When I speak of deformations of isolated singular points on algebraic schemes, the basic setup is as follows:

$\pi : X \to Y$ <u>is a morphism of schemes</u>, Y <u>is a noetherian scheme</u>, π <u>is of finite type and flat</u>, $\varepsilon : Y \to X$ <u>is a morphism such that</u> $\pi \circ \varepsilon$ = <u>identity</u>, π <u>is smooth on</u> $X - \varepsilon(Y)$, <u>and all the fibres</u> $X_y = \pi^{-1}(y)$, $y \in Y$, <u>are reduced and equidimensional</u> (i.e., all the irreducible components of X_y have the same dimension). Here the word "<u>smooth</u>" means that if x is any point of $X - \varepsilon(Y)$ then (assuming that Y is affine, say Spec(A), without any loss of generality) π is decomposed into an étale morphism from a neighborhood of x in X to <u>Spec</u>$(A[t_1, \ldots, t_n])$ and the projection from this spectrum to $Y = \mathrm{Spec}(A)$, where n = the dimension of the fibres of π. It follows from the assumptions, that the fibre X_y for each $y \in Y$ is non-singular, except for the possible singularity at $\varepsilon(y) \in X_y$. Thus we have a family of algebraic schemes with (possible) isolated singular points, $\{(X_y, \varepsilon(y))\}$, which are parametrized by the points of Y. If Y is a non-singular curve, then the flatness of π means simply that every irreducible component of X is surjectively mapped to Y. In general, it implies that all the fibres X_y, $y \in Y$, have the same dimension and that every irreducible component of X is surjectively mapped to a connected component of Y.

In this basic setup, we do not lose too much by taking "algebraic varieties, say, over an algebraically closed field" instead of "schemes". However, we need to consider some other "derived" setups, such as truncations and completions of the given family, in which "schemes with nilpotent elements in the structure sheaves" and "formal schemes" are involved.

Suppose a family (of isolated singularities), (π, X, Y, ε), is given as above. Let $\underline{I}$ be the ideal sheaf of the subscheme $\varepsilon(Y)$ in $\underline{O}_X$. We write then $X_{(\nu)}$ for the subscheme of X defined by the ideal sheaf $\underline{I}^{\nu+1}$, where ν is any non-negative integer. $X_{(0)} = \varepsilon(Y)$ and all the $X_{(\nu)}$, $\nu \geq 0$, have the same underlying topological space. The structure sheaf of $X_{(\nu)}$ is $\underline{O}_X/\underline{I}^{\nu+1}$ (restricted to its support). We have a canonical immersion $X_{(\nu)} \to X_{(\mu)}$ for $\mu > \nu$, and we call the limit space $\hat{X} = \varinjlim_{\nu} X_{(\nu)}$ the $\underline{I}$-adic completion of X. The structure sheaf of this "formal scheme" $\hat{X}$ is $\varprojlim_{\nu} \underline{O}_X/\underline{I}^{\nu+1}$. The morphism $\pi: X \to Y$ (resp. $\varepsilon: Y \to X$) induces morphisms $\pi_{(\nu)}: X_{(\nu)} \to Y$ and $\hat{\pi}: \hat{X} \to Y$ (resp. $\varepsilon_{(\nu)}: Y \to X_{(\nu)}$ and $\hat{\varepsilon}_{(\nu)}: Y \to \hat{X}$). The "derived" family $(\pi_{(\nu)}, X_{(\nu)}, Y, \varepsilon_{(\nu)})$ (resp. $(\hat{\pi}, \hat{X}, Y, \hat{\varepsilon})$) will be called the ν-th truncation (resp. the completion) of the given (π, X, Y, ε).

In what follows, the main theme is to compare a family (π, X, Y, ε) with another $(\pi', X', Y, \varepsilon')$ (likewise, their truncations, or their completions), where the parameter space Y is the same for all. By abuse of language, I shall say, for instance, that

$$\varphi_{(\nu)}: (\pi_{(\nu)}, X_{(\nu)}, Y, \varepsilon_{(\nu)}) \to (\pi'_{(\nu)}, X'_{(\nu)}, Y, \varepsilon'_{(\nu)})$$

is a morphism (or an isomorphism) within a neighborhood of a point $y \in Y$, when $\varphi_{(\nu)}$ is meant to be a morphism (or an isomorphism) from

$\pi_{(\nu)}^{-1}(U)$ to $\pi'^{-1}_{(\nu)}(U)$ such that $\pi'_{(\nu)} \circ \varphi_{(\nu)} = \pi_{(\nu)}$, where U is a certain neighborhood of the point y in Y.

Theorem 1. Let (π, X, Y, ε) *be a family of isolated singular points (in the sense described above). Let* y *be a point of* Y. *Then there exists a pair of integers* (t, r), $t \geqq 1$ *and* $r \geqq 0$, *which has the following properties*

(I) *Let* ν *be an integer not less than* t, and $(\pi', X', Y, \varepsilon')$ *any family of isolated singular points. Suppose* $\dim(X_y) = \dim(X'_y)$ *and there is given an isomorphism* $\varphi_{(\nu)}: (\pi'_{(\nu)}, X'_{(\nu)}, Y, \varepsilon'_{(\nu)}) \xrightarrow{\approx} (\pi_{(\nu)}, X_{(\nu)}, Y, \varepsilon_{(\nu)})$ *within a neighborhood of* y. Then the isomorphism

$\varphi_{(\nu-r)}: (\pi'_{(\nu-r)}, X'_{(\nu-r)}, Y, \varepsilon'_{(\nu-r)}) \xrightarrow{\approx} (\pi_{(\nu-r)}, X_{(\nu-r)}, Y, \varepsilon_{(\nu-r)})$, *induced by* $\varphi_{(\nu)}$, *extends to an isomorphism* $\hat{\varphi}: (\hat{\pi}', \hat{X}', Y, \hat{\varepsilon}') \xrightarrow{\approx} (\hat{\pi}, \hat{X}, Y, \hat{\varepsilon})$ *within a neighborhood of* y.

(II) *If* $h: \tilde{Y} \to Y$ *is any morphism of noetherian schemes and* $\tilde{y}$ *is any point of* $\tilde{Y}$ *such that* $h(\tilde{y}) = y$, *then the pair of integers* (t, r) *has the same property as* (I) *for the family* $(\tilde{\pi}, \tilde{X}, \tilde{Y}, \tilde{\varepsilon})$ *obtained from* (π, X, Y, ε) *by the base extension* h, *and for the point* $\tilde{y}$ *of* $\tilde{Y}$, *where* $\tilde{X} = X \times_Y \tilde{Y}$, $\tilde{\pi} = \pi \times_Y \tilde{Y}$, $\tilde{\varepsilon} = \varepsilon \times_Y \tilde{Y}$.

In particular, I shall consider the case in which X is an algebraic k-scheme, with a field k, and Y is a geometric point of X with value in k (or, a k-rational point). In this case, the theorem asserts, roughly speaking, that *the analytic structure of the isolated singular point* Y *of* X *is determined by* $\dim X$ *and by the structure of the truncated local algebra* $\underline{\underline{O}}_Y / \underline{m}_Y^{t+1}$, where $\underline{\underline{O}}_Y$ = the local ring of X at Y and $\underline{m}_Y$ the maximal ideal of $\underline{\underline{O}}_Y$.

Definition 1. For a family of isolated singular points (π, X, Y, ε) and a point y of Y, I call (t, r) a pair of TR-indices of (π, X, Y, ε) at the point y, if it has the properties (I) and (II) stated in Theorem 1. In particular, when an algebraic k-scheme X is given with an isolated singular point y (with value in k), (t, r) will be called a pair of TR-indices of (X, y) (or, that of the isolated singular point y of X).

Note that if (t, r) is a pair of TR-indices of (π, X, Y, ε) then so is every pair of integers $(\bar{t}, \bar{r})$ such that $\bar{t} \geqq t$ and $\bar{r} \geqq r$. It can be proved that the integer r can be zero only if $\varepsilon(y)$ is a simple point of X_y.

The theorem has an obvious "complex-analytic" analogue, in which X and Y are complex-analytic spaces with holomorphic maps π and ε. In the complex-analytic case, one can find a proof of the theorem (for an isolated singular point $Y = y$) in HIRONAKA-ROSSI, [3], which is based on desingularization techniques (HIRONAKA, [2]; especially, Corollary 1, p. 153, § 7, Chap. 0) and infinitesimal calculus due to Grothendieck-Grauert. In this case, Grauert's normal projection method ([1], Satz 5, p. 359) gives a stronger conclusion in which the extended isomorphism $\hat{\varphi}$ of the theorem is holomorphic (or, to be precise, $\hat{\varphi}$ is the formalization of a biholomorphic map from a neighborhood of $\varepsilon'(y)$ in X' to a neighborhood of $\varepsilon(y)$ in X). It was then pointed out by M. Artin that the normal projection method provides an étale equivalence (which implies a holomorphic one in the complex case) instead of the formal equivalence $\hat{\varphi}$. On the other hand, I found a new proof of the theorem (which works in the above-stated generality; for instance, in any characteristic case) and by these means, I obtained a theorem of the following type.

Theorem 2. Let (π, X, Y, ε) and $(\pi', X', Y, \varepsilon')$ be families of isolated singular points, and y a point of Y. Suppose there is given an isomorphism $\hat{\varphi}: (\hat{\pi}', \hat{X}', Y, \hat{\varepsilon}') \xrightarrow{\approx} (\hat{\pi}, \hat{X}, Y, \hat{\varepsilon})$ within a neighborhood of y in Y. Let ν be any positive integer. Then, within a neighborhood of y, there exist etale morphisms $\lambda: (\tilde{\pi}, \tilde{X}, Y, \tilde{\varepsilon}) \longrightarrow (\pi, X, Y, \varepsilon)$ and $\lambda': (\tilde{\pi}', \tilde{X}', Y, \tilde{\varepsilon}') \longrightarrow (\pi', X', Y, \varepsilon')$, which induce isomorphisms of completions, and there exists an isomorphism $\tilde{\varphi}: (\tilde{\pi}', \tilde{X}', Y, \tilde{\varepsilon}') \xrightarrow{\approx} (\tilde{\pi}, \tilde{X}, Y, \tilde{\varepsilon})$ which induces the same isomorphism $\varphi_{(\nu)}: (\pi'_{(\nu)}, X'_{(\nu)}, Y, \varepsilon'_{(\nu)}) \xrightarrow{\approx} (\pi_{(\nu)}, X_{(\nu)}, Y, \varepsilon_{(\nu)})$ as the given $\hat{\varphi}$ does.

In this theorem, étale morphisms are meant to be those of finite type. In my proof, this theorem and the preceding one are proven simultaneously. It should be interesting to find a direct proof of the second theorem and to look into the question of whether it is essential or not to assume the smoothness of $\pi: X \longrightarrow Y$ for all points of $X - \varepsilon(Y)$. (Note that this smoothness assumption is essential in the first theorem.)

Let us now go back to investigate further the notion of TR - indices of a family of isolated singular points.

Theorem 3. Let (π, X, Y, ε) be a family of isolated singluar points and y a point of Y. Let (t, r) be a pair of TR - indices of (π, X, Y, ε) at y. Then there exists a neighborhood U of y in Y such that for every point z of U, (t, r) is a pair of TR - indices for the isolated singular points $(X_z, \varepsilon(z))$, where $X_z = \pi^{-1}(z)$.

The converse of the theorem is far from being true. Namely, let us introduce the notion of TR - <u>indices of all "near-by" fibres of a family</u> (π, X, Y, ε) at a point y of Y. This is any pair of integers $(\bar{t}, \bar{r})$, $\bar{t} \geqq 1$ and $\bar{r} \geqq 0$, such that there exists a neighborhood U of y in Y such that $(\bar{t}, \bar{r})$ is a pair of TR - indices of the fibres $(X_z, \varepsilon(z))$ for all $z \in U$. Then the claim is that $(\bar{t}, \bar{r})$ is not in general a pair of TR - indices of (π, X, Y, ε) at y.

The difference between the above two notions of TR - indices for a family, namely (t, r) and $(\bar{t}, \bar{r})$, can be seen in the following two theorems, the first of "affirmative nature" and the second of "negative nature".

Let us start with a fixed isolated singular point of an algebraic k - scheme (X_0, x_0). Let us then consider various families of isolated singular points (π, X, Y, ε) with <u>center</u> (X_0, x_0); that is to say, there is a specified point y_0 of Y and an isomorphism $\hat{\varphi}_0 : (\hat{X}_0, x_0) \xrightarrow{\approx} (\hat{X}y_0, \varepsilon(y_0))$, where $\hat{X}_0$ (resp. $\hat{X}y_0$) denotes the completion of X_0 (resp. Xy_0) by the powers of the maximal ideal at x_0 (resp. the same at $\varepsilon(y_0)$).

<u>Theorem 4. Given an isolated singular point</u> (X_0, x_0), <u>there exists a pair of integers</u> $(\bar{t}, \bar{r})$ <u>such that if</u> (π, X, Y, ε) <u>is any family of isolated singular points with center</u> $(\hat{X}_0, x_0) \xrightarrow{\approx} (\hat{X}y_0, \varepsilon(y_0))$, <u>then there exists a neighborhood</u> U <u>of</u> y_0 <u>in</u> Y <u>and</u> $(\bar{t}, \bar{r})$ <u>is a pair of</u> TR - <u>indices for all fibres</u> $(Xy, \varepsilon(y))$ <u>with</u> $y \in U$.

<u>Theorem 5. Suppose</u> (X_0, x_0) <u>is an isolated singular point of a complete intersection</u> X_0, <u>i.e., there exists a local imbedding of</u> X_0 <u>in an affine</u> N - <u>space so that the local ideal of</u> X_0 <u>at</u> x_0 <u>is generated by</u> $(N - \dim X_0)$ <u>elements. Suppose</u> x_0 <u>is not a simple point of</u> X_0. <u>Then, for every pair of</u>

<u>integers</u> (t, r), <u>there exists a family of isolated singular points</u> (π, X, Y, ε) <u>with center</u> $(\hat{X}_0, x_0) \xrightarrow{\approx} (\hat{X}y_0, \varepsilon(y_0))$, <u>such that</u> (t, r) <u>is not a pair of</u> TR-<u>indices of</u> (π, X, Y, ε) <u>at</u> y_0.

Let us remark that if (π, X, Y, ε) is a family of isolated singular points and Xy is a complete intersection at $\varepsilon(y)$ for some $y \in Y$, then there exists a neighborhood U of y in Y so that all the fibres X_z is a complete intersection at $\varepsilon(z)$ for all $z \in U$. In fact, X itself is a complete intersection locally at $\varepsilon(y)$ in <u>Spec</u> $(A[t_1, \ldots, t_N])$ with independent variables t_j $(1 \leqq j \leqq N)$, where $y \in$ <u>Spec</u> $(A) \subseteqq Y$.

In dealing with complete intersections, there is another point that makes "deformation theory" simpler than the general case. Namely, let $\pi: X \to Y$ be any flat morphism of finite type, say with a regular noetherian scheme Y, and $\varepsilon: Y \to X$ is a section, i.e., a morphism such that $\pi \circ \varepsilon =$ identity. Suppose that for every point $y \in Y$, the fibre Xy is reduced and equidimensional and $\varepsilon(y)$ is an isolated singular point of Xy. Notice that such (π, X, Y, ε) is a <u>"family" of isolated singular points</u> (in the sense of this paper) under only one additional condition that $X - \varepsilon(Y)$ is smooth over Y. This condition means that $Xy - \varepsilon(y)$ is non-singular for all $y \in Y$. Now the point is that if all the fibres Xy are complete intersections then we can always modify (π, X, Y, ε) into another $(\overline{\pi}, \overline{X}, Y, \overline{\varepsilon})$, satisfying the additional condition, in such a way that there exists an isomorphism $(\overline{\pi}_{(\nu)}, \overline{X}_{(\nu)}, Y, \overline{\varepsilon}_{(\nu)}) \xrightarrow{\approx} (\pi_{(\nu)}, X_{(\nu)}, Y, \varepsilon_{(\nu)})$ where (ν, μ) for some μ is a pair of TR-indices for all the isolated singular points $(Xy, \varepsilon(y))$, $y \in Y$.

Let us furthermore remark that the existence of $(\overline{t}, \overline{r})$ in Theorem 4 suggests that:

The totality of all near-by isolated singularities of a given one is "of finite type" in sone algebro - geometric sense.

The meaning of such a statement can be made very precise in the case of complete intersections. Namely, let me introduce the notion of "quasi - equivalent" families. This is as follows. Let (π, X, Y, ε) and $(\pi', X', Y, \varepsilon')$ be two families of isolated singular points, having the same parameter space Y. Then I say that they are quasi - equivalent, if there exists an isomorphism $(\pi'_{(\nu)}, X'_{(\nu)}, Y, \varepsilon'_{(\nu)}) \xrightarrow{\approx} (\pi_{(\nu)}, X_{(\nu)}, Y, \varepsilon_{(\nu)})$, where (ν, μ) for some μ is a pair of TR - indices for all the fibres $(Xy, \varepsilon(y))$ and $(X'y, \varepsilon'(y))$, $y \in Y$. Now, I claim that Theorem 4 implies, for instance, that, if (X_0, x_0) is a complete intersection, then there exists a family of isolated singular points $(\pi^*, X^*, Y^*, \varepsilon^*)$ with center $(\hat{X}_0, x_0) \xrightarrow{\approx} (\hat{X}^* y_0, \varepsilon^*(y_0))$ which induces every other family of isolated singular points with the same center, "up to quasi - equivalences" within some neighborhoods of the center.

Theorem 5, on the other hand, implies that there exists no family of isolated singular points with center $(\hat{X}_0, x_0)$ which induces every other family of isolated singular points with the same center, "up to formal equivalences" (or, up to isomorphisms of completions) within suitable neighborhoods of the center.

These facts attract me towards the question of finding "reasonable and (or) significant restrictions" to be imposed on families involved, which enable us to construct "a local universal family up to formal equivalences". For instance, the question leads me to the notion of "equi - singularity". A theory of equi-singularity has been dug up by Zariski and is gradually showing up its clear face in some special cases. But it seems that a full and complete theory is at present utterly out of sight.

Zariski's theory of equi-singularity is strictly concerned with "hypersurfaces". Here I like to propose a notion of equi-singularity which applies even to non-hypersurface cases, although the characteristic of the base field is required to be zero as in Zariski's case.

Definition 2. Let X be an algebraic scheme over a field k of characteristic zero. Assume that X is reduced and equi-dimensional. Let Y be a non-singular irreducible subscheme of X. Let y be a point of Y. Then I say that X is equi-singular along Y at the point y, if (replacing X, and Y accordingly, by a neighborhood of y) there exists a morphism $\pi : X \to Y$ which has the following properties:

i) (π, X, Y, ε) is a family of isolated singular points (in the sense described at the very beginning), where $\varepsilon : Y \to X$ denotes the canonical immersion, and

ii) let $\mathcal{J}_0$ be the sheaf of Jacobian ideals of (π, X, Y, ε) (see below) and $\mathcal{I}$ the sheaf of ideals defining Y on X. Take the sheaf of product ideals, $\mathcal{J} = \mathcal{J}_0\mathcal{I}$, on X, and the composition $\tilde{h} : \tilde{X} \to X$ of the birational blowing-up of X by the ideals $\mathcal{J}$ and the normalization of the blown-up scheme. Let $\tilde{\mathcal{J}} = \mathcal{J}\underline{O}_{\tilde{X}}$, the ideal sheaf on $\tilde{X}$ generated by $\mathcal{J}$. Then $\underline{O}_{\tilde{X}}/\tilde{\mathcal{J}}$ is flat over $\underline{O}_Y$, or, the subscheme $\tilde{Y}$ of $\tilde{X}$ defined by $\tilde{\mathcal{J}}$ is flat over Y with reference to the morphism $\pi \circ \tilde{h}$.

The sheaf of Jacobian ideals of (π, X, Y, ε) is defined as follows:

For each point $y \in Y$, by replacing X by a suitable neighborhood of $\varepsilon(y)$ (and accordingly Y), I assume that there exists an imbedding $p: X \to \underline{\mathrm{Spec}}\,(A[T_1, T_2, \ldots, T_N])$, where $Y = \underline{\mathrm{Spec}}\,(A)$ and T_j $(1 \leqq j \leqq N)$ are independent variables, such that $\pi = (\text{projection}) \circ p$ and the ideal of $(p \circ \varepsilon)(Y)$ is generated by $T_1, T_2, \ldots, T_N$. Then the sheaf of Jacobian ideals $\mathcal{J}_0$ on X is generated by $(N - \underline{\dim}\, X_y) \times (N - \underline{\dim}\, X_y)$ - minors of the Jacobian matrix $\partial(f_1, \ldots, f_m)/\partial(T_1, \ldots, T_N)$, where $(f_1, \ldots, f_m)$ is a base of the ideal of $p(X)$ in $A[T]$. It is important that the sheaf $\mathcal{J}_0$ is independent of the choice of imbedding p.

Remark. If the condition i) of Definition 2 is satisfied, then the condition ii) is equivalent to the following:

ii*) $\tilde{\mathcal{J}}^{\nu}/\tilde{\mathcal{J}}^{\nu+1}$ is flat over $\underline{O}_Y$ for all integers $\nu \geqq 0$.

Moreover, if $\underline{\dim}\, Y = 1$, then it is equivalent to:

ii**) Every irreducible component of $\tilde{h}^{-1}(\varepsilon(Y))$ is mapped onto a connected component of Y by $\pi \circ \tilde{h}$.

The following theorem suggests the possibility that the totality of all small families of isolated singular points with a given center can be derived from a certain universal family so long as they are subject to some equi-singularity condition.

Theorem 6. Let (X_0, x_0) be an isolated singular point. Then there exists a pair of integers (t, r) such that for every family of isolated singular points (π, X, Y, ε) with center $(\hat{X}_0, x_0) \cong (\hat{X}_{y_0}, \varepsilon(y_0))$, (t, r) is a pair of TR - indices of (π, X, Y, ε) at y_0 provided (π, X, Y, ε) satisfies the condition ii) of Definition 2.

It seems to me that Theorem 6 remains true if one replaces the condition ii) of Definition 2 by some reasonably weaker condition.

The condition ii) of Definition 2 has some geometric and topological significances. From now on, this condition will be referred to as "condition (ES)". I take now the case in which the base field k is the complex number field $\mathbb{C}$. In the place of "schemes", I shall take "complex-analytic varieties". Notice that the "condition (ES)" has an obvious analogue in the complex-analytic case. Let (X_0, x_0) be an isolated singular point, where X_0 is now a complex-analytic variety (reduced and equi-dimensional Suppose we have a local imbedding $p_0 : X_0 \to \mathbb{C}^N$, $\mathbb{C}^N$ = the complex number space of dimension N. For simplicity, assume that $p_0(x_0) = 0$, the origin. Let $T_x(X_0)$ be the complex tangent space of X_0 at $x \in X_0$, $\neq x_0$, which is realized as a linear subspace of $\mathbb{C}^N$ in a natural manner. If $u = (u_1, u_2, \ldots, u_N)$ and $v = (v_1, v_2, \ldots, v_N)$ are two vectors in C^N, then $u \cdot v$ denotes the inner product $\sum_{i=1}^N u_i \cdot \overline{v_i}$. For a point $x \in X_0$, let $\overrightarrow{0x}$ denote the vector in $\mathbb{C}^N$ which ends at x (and, as always, starts from the origin). Consider the following real-valued function of $x \in X_0 - \{x_0\}$,

$$\tau(p_0; x) = \max_{\substack{v \in T_x(X_0) \\ v \neq 0}} \left\{ \frac{|v \cdot \overrightarrow{0x}|}{|v|\,|\overrightarrow{0x}|} \right\}$$

where $|v|$ = the length of $v = \sqrt{\sum_{i=1}^N |v_i|^2}$. Then, Whitney proves:

<u>Theorem</u> 7.

$$\lim_{x \to 0} \tau(p_0; x) = 1 .$$

By this theorem, if we set $\tau(p_0; x_0) = 1$, then $\tau(p_0; x)$ becomes a continuous function on X_0. Suppose there is given a family of isolated singular points $(\pi, X, Y, \mathcal{E})$. Then, at least locally, one can find an imbedding of the form $p: X \rightarrow Y \times \mathbb{C}^N$ such that $\pi = (\text{projection}) \circ p$ and $(p \circ \mathcal{E})(Y) = Y \times 0$. Let me say that such an imbedding p is permissible. Pick one permissible imbedding p. Then, for each point $y \in Y$, p induces an imbedding $p_y: Xy \rightarrow \mathbb{C}^N$ $(= y \times \mathbb{C}^N)$. For this induced imbedding p_y, I have a continuous real-valued function $\tau(p_y; x)$, $x \in Xy$. Let us define a real-valued function on X as follows:

$$\tau(p; x) = \tau(p_y; x) \quad \text{if} \quad x \in Xy, \quad y \in Y.$$

I shall call such a function $\tau(p; x)$ a W-function for the family of isolated singular points (π, X, Y, ε). This function depends upon the choice of imbedding p. I shall say that the W-function $\tau(p; x)$ is associated with the imbedding p. One can prove that, given a family of isolated singular points (π, X, Y, ε), if a W-function associated with a permissible imbedding is continuous on X, then the same holds for every permissible imbedding. In view of this fact, we can speak of the continuity of W-function for a given $(\pi, X, Y, \mathcal{E})$ without asking if X admits a global imbedding $X \rightarrow Y \times \mathbb{C}^N$ for some N, because X admits a permissible imbedding at least locally at every point of $\varepsilon(Y)$.

In view of the theorem of Whitney (or, some other reasons), given an isolated singular point (X_0, x_0) with an imbedding $p_0: X_0 \rightarrow \mathbb{C}^N$ with $p_0(x_0) = 0$, one can find a real number $\rho > 0$ such that if $0 < \mathcal{E} < \rho$, then X_0 is transversal to the sphere in $\mathbb{C}^N$ with center 0 and with radius $\mathcal{E}$; this sphere $S_\mathcal{E}$ has real dimension $2N-1$. Such a real number ρ will be called a permissible radius of (X_0, x_0) with p_0. Hence $W_\mathcal{E} = X_0 \cap S_\mathcal{E}$ is a manifold of dimension $2n-1$, where $n = \dim X_0$. If we identify S_ε with a standard $(2N-1)$-sphere S, then the imbedding $W_\varepsilon \to S$ is a differentiable isotopy in terms of the parameter ε $(0 < \varepsilon \leqq \rho)$. Let us simply write W for W_ε, and the isotopy class (W, S) is the "topology" of the singular point (X_0, x_0) with imbedding p_0. A family (π, X, Y, ε) with a permissible imbedding $p: X \to Y \times \mathbb{C}^N$ will be said to be topologically stable if for every point $\bar{y}$ of Y, there exists a neighborhood U of $\bar{y}$ in Y and a positive real number ρ such that ρ is a permissible radius of $(Xy, \varepsilon(y))$ with the induced imbedding $p_y: Xy \to \mathbb{C}^N$ for all $y \in U$.

I can prove:

Theorem 8. Given a family of isolated singular points (π, X, Y, ε) with a non-singular irreducible Y and with a permissible imbedding $p: X \to Y \times \mathbb{C}^N$,

(I) the condition (ES) $\Rightarrow$ the continuity of W-function $\Rightarrow$ the topological stability;

(II) if $\dim Xy = 1$ for $y \in Y$, then the continuity of W-function $\Rightarrow$ the order of singularity $\delta(Xy, \varepsilon(y))$ is constant for $y \in Y$. ($\delta(Xy, \varepsilon(y)) = \dim_C \tilde{O}/O$, where O = the local ring of Xy at $\varepsilon(y)$ and $\tilde{O}$ = the integral closure of O in the total ring of fractions of O, both being viewed as vector spaces over C.);

(III) if $\dim Xy = 1$ for $y \in Y$ and $N = 2$ (i.e., the case of plane curves), there is a complete equivalence of various conditions, namely, the condition (ES) $\Rightarrow$ the continuity of W-function $\Rightarrow$ the topological stability $\Rightarrow$ the condition (ES).

References

[1] H. GRAUERT, Über Modificationen und exceptionelle analytische Mengen, Math. Ann., 146, pp. 331-368 (1962)

[2] H. HIRONAKA, Resolution of singularities of an algebraic variety over a field of characteristic zero, Ann. of Math., 79, pp. 109-326 (1964)

[3] H. HIRONAKA - H. ROSSI, On the equivalence of imbeddings of exceptional complex spaces, forthcoming in Math. Ann.

EQUISINGULARITY AND RELATED QUESTIONS OF CLASSIFICATION OF SINGULARITIES.

by

O. Zariski

§1. The elusive idea of equivalent singularities.

Ideally, a complete theory of equivalence of singularities must give a precise meaning to a statement such as this: "the singularity which a given variety V has at a given point P is "the same" as the singularity which another given variety V' has at a given point P'". In addition, the theory must include a number of criteria of equivalence, whether algebraic or algebro-geometric in nature; or topological, if we are dealing with the complex domain. Naturally, one will impose some restrictions on the ground field k, say k will be assumed to be algebraically closed and even--to begin with-- of characteristic zero.

It goes without saying that the equivalence relation which we are lookking for is one which is much weaker than strict analytical equivalence (i.e., isomorphism of the completions of the local rings of P and P'). Each class of equivalent algebroid singularities will give rise to a variety of biholomorphic moduli (the quotient space of that class, modulo analytic equivalence). One should not expect, however, that the variety of moduli in this context will be irreducible, or even equidimensional. Examples to the contrary can already be given in the case of singularities of algebroid plane curves.

Similarly, if we are in the complex domain, we envisage an equivalence relation which is much stronger than topological equivalence of the two varieties V and V', locally at P and P' respectively. Thus, if V is an algebroid plane curve, the only topological invariant of V is the number of irreducible analytical brancheswhich V has at the point P. However, if we deal only with normal points, then one can expect that in this case the relationship between topological equivalence and algebro-geometric equivalence will be much less casual than in the general case. The only non-trivial result which we have in this connection is Mumford's theorem that if an algebraic surface is topologically a manifold at a normal point then that point is a simple point of the surface.

Still with reference to the complex domain, the set-up in regard to the connection between topological equivalence and the (hypothetical) algebro-geometric equivalence, changes radically if our varieties V and V' are embedded varieties, i.e., are varieties of dimension r, embedded (locally at P and P' respectively) in affine (r + 1)-spaces A, A', and if we look at the complementary spaces A - V, A' - V'. Then one may conjecture that P and P' are equivalent singularities if and only if the spaces A - V and A' - V' are homeomorphic (locally at P and P'). This is only known to be true in the case r = 2.

§2. The case of plane algebroid curves.

This classical case, in which everything concerning equivalence is well-known, is nevertheless a very important case, because it contains the germ of all possible generalizations. One must, however, have a second look at this classical case, using a somewhat more sophisticated approach than the one used by Noether and Enriques in their study of the composition of singularities. Above all, one must devise in this case a definition of equivalence which does not presuppose a detailed analysis of the singularity, for in the higher dimensional case such an analysis is a hopeless undertaking. Let me give you three such definitions and say that it can be proved that they are all equivalent (the proofs are not completely trivial) We assume throughout that the ground field k is algebraically closed (of arbitrary characteristic) .

If C is an algebroid plane curve, with origin P we denote by $m_P(C)$ the multiplicity of the point P . If $p_1, p_2, \ldots, p_t$ are the distinct tangents of C at P ($t \leq m_P(C)$) , then we denote by C_ν ($\nu = 1, 2, \ldots, t$) the union of all irreducible branches of C which are tangent to p_ν, and we call $C_1, C_2, \ldots, C_t$ the tangential components of C .

Let D be another plane algebroid curve, with some origin Q . We assume that C and D have the same number h of irreducible branches, and we denote by $\delta_1, \delta_2, \ldots, \delta_h$ the irreducible branches of D.

DEFINITION . A (1,1) mapping π of the set of branches $\gamma_1, \gamma_2, \ldots, \gamma_h$ of C onto the set of branches $\delta_1, \delta_2, \ldots, \delta_h$ of D is said to be a tangentially stable pairing $\pi : C \longrightarrow D$ between the branches of C and those of D, if the following condition is satisfied: given any two branches γ_i and γ_j of C, the corresponding branches $\pi(\gamma_i)$ and $\pi(\gamma_j)$ of D have the same tangent if and only if γ_i and γ_j have the same tangent.

Assume that there exists a tangentially stable pairing $\pi : C \longrightarrow D$ between the branches of C and the branches of D. Then it is clear that C and D have the same number t of distinct tangent lines and that π induces a (1,1) mapping of the set $\{p_1, p_2, \ldots, p_t\}$ of tangent lines of C onto the set $\{q_1, q_2, \ldots, q_t\}$ of tangent lines of D. We choose our indexing of these tangent lines in such a way that p_ν and q_ν are paired in this induced mapping, and we denote by C_ν (resp. D_ν) the tangential component of C (resp., D) associated with p_ν (resp., q_ν). Then it is clear that for each $\nu = 1, 2, \ldots, t$, $\pi_\nu : C_\nu \longrightarrow D_\nu$ of the set of branches of C_ν onto the set of branches of D_ν (the pairing π_ν is trivially tangentially stable, since both C_ν and D_ν have only one tangent line).

Assume that there exists a tangentially stable pairing $\pi : C \longrightarrow D$ between the branches of C and the branches of D. Then it is clear that C and D have the same number t of distinct tangent lines and that π induces a $(1,1)$ mapping of the set $\{p_1, p_2, \ldots, p_t\}$ of tangent lines of C onto the set $\{q_1, q_2, \ldots, q_t\}$ of tangent lines of D. We choose our indexing of these tangent lines in such a way that p_ν and q_ν are paired in this induced mapping, and we denote by C_ν (resp. D_ν) the tangential component of C (resp., D) associated with p_ν (resp., q_ν). Then it is clear that for each $\nu = 1, 2, \ldots, t$, π induces a $(1,1)$ mapping $\pi_\nu : C_\nu \longrightarrow D_\nu$ of the set of branches of C_ν onto the set of branches of D_ν (the pairing π_ν is trivially tangentially stable, since both C_ν and D_ν have only one tangent line).

Let π and π_ν be as above (π-tangentially stable), let T be a locally quadratic transformation with center at the origin of P of C and let S be a locally quadratic transformation with center at the origin Q of D. Let $C' = T(C)$, $C'_\nu = T(C_\nu)$, $D' = S(D)$, $D'_\nu = S(D_\nu)$ be the proper transforms. It is clear that π_ν induces a $(1,1)$ mapping π'_ν of the set of branches of C'_ν onto the set of branches of D'_ν. Namely, if we assume that the branches of C and D have been so indexed that $\pi(\gamma_i) = \delta_i$, for $i = 1, 2, \ldots, h$, then we set $\pi'_\nu(\gamma'_i) = \delta'_i$, where $\gamma'_i = T(\gamma_i)$ and $\delta'_i = S(\delta_i)$. The pairing

$\pi'_\nu / C'_\nu \longrightarrow D'_\nu$ between the branches of C'_ν and the branches of D'_ν is, however, not necessarily tangentially stable.

An algebroid curve C is <u>regular</u> if its origin P is a simple point of C, i.e., if $m_P(C) = 1$. If P is a <u>singular</u> point (i.e., if $m_P(C) > 1$), then we can resolve the singularity of C at P by a finite number of locally quadratic transformations. By a sequence of <u>successive quadratic transforms of</u> C we mean a sequence $\{C, C', C'', \ldots, C^{(i)}, \ldots\}$ of algebroid curves $C^{(i)}$ such that for each i, $C^{(i+1)}$ is a connected component of the proper transform of $C^{(i)}$ under a locally quadratic transformation whose center is the origin of $C^{(i)} (C^{(0)} = C)$. The fact that the singularity of C can be resolved can then be stated as follows: there exists an integer N such that in <u>any</u> sequence of successive quadratic transforms of C, the curves $C^{(i)}$ are regular if $i \geqq N$. We denote by $\sigma(C)$ the smallest integer N with the above property ($\sigma(C) = 0$ if and only if C itself is a regular curve).

It is clear that if $C'_1, C'_2, \ldots, C'_t$ are the connected components of the proper quadratic transform $T(C)$ of C, and if $\sigma(C) > 0$, then $\sigma(C'_\nu) < \sigma(C)$ for $\nu = 1, 2, \ldots, t$. Our first definition of equivalence of algebroid curves proceeds by induction on $\sigma(C)$.

Let $\pi / C \longrightarrow D$ be a pairing between the branches of C and the branches of D (it is already assumed that C and D have the same number h of branches). If C is regular (whence $\sigma(C) = 0$), then C (and therefore also D) has only one branch, $\pi : C \longrightarrow D$ is uniquely determined, and we say that π is an <u>(a)-equivalence</u> if also D is a regular curve. Assume that for all pairs of algebroid curves Γ, Δ with the same number of branches and such that $\sigma(\Gamma) < \sigma(C)$ it has already been defined what is to be meant by saying that a pairing $\Gamma \longrightarrow \Delta$ between the branches of Γ and the branches of Δ is an (a)-equivalence. Then we define an (a)-equivalence between C and D as follows (we use the notations introduced earlier in this section):

DEFINITION 1. <u>An</u> (a)-<u>equivalence</u> $\pi : C \longrightarrow D$ <u>is a pairing</u> π <u>between the branches of</u> C <u>and the branches of</u> D <u>having the following properties:</u>

1) π <u>is tangentially stable.</u>

2) <u>If</u> $\delta_i = \pi(\gamma_i)$ $(i = 1, 2, \ldots, h)$, <u>then</u> $m_P(\gamma_i) = m_Q(\delta_i)$.

3) <u>The pairing</u> $\pi'_\nu : C'_\nu \longrightarrow D'_\nu$ $(\nu = 1, 2, \ldots, t)$ <u>is an</u> (a)-<u>equivalence.</u>

We now proceed to our second definition of equivalence between algebroid singularities. If T is our quadratic transformation, with center P then T blows up P into the line $x' = 0$ of the (x', y')-plane. We denote this line by $\mathcal{E}'$ and we refer to $\mathcal{E}'$ as the <u>exceptional curve</u> of T. If C_ν is a tangential component of C and $C'_\nu = T(C_\nu)$

is the proper T-transform of C_ν, then $\mathcal{E}'$ contains the origin P'_ν of C'_ν, but $\mathcal{E}'$ is not a component of C'_ν. We denote by C'^*_ν the algebroid curve $C'_\nu \cup \mathcal{E}'$ and we call C'^*_ν the <u>total</u> T-transform of C_ν; in symbols: $C'^*_\nu = T\{C_\nu\}$. We set $C'^* = T(C) \cup \mathcal{E}'$ and we call C'^* the <u>total</u> T-transform of C. Note that $m_{P_\nu}(C'^*_\nu)$ is always $\geqq 2$.

It is known that after a finite number of successive quadratic transformations one can reach a stage where the <u>total</u> transform of C <u>has only ordinary double points.</u> More precisely: there exists an integer $N \geqq 0$ (depending on C) with the following property: if $\{C, C'^*, C''^*, \ldots, C^{(}$ is <u>any</u> sequence of algebroid curves such that for any i we have $C^{(i+1)*} = C^{(i+1)} \cup \mathcal{E}^{i+1}$, where $C^{(i+1)}$ is a connected component of the proper quadratic transform $T^{(i)}(C^{(i)})$ of $C^{(i)}$ ($T^{(i)}$ being a quadratic transformation with center at the origin $P^{(i)}$ of $C^{(i)}$) and $\mathcal{E}^{(i+1)}$ is the exceptional curve of $T^{(i)}$, then for $i \geqq N$ the origin $P^{(i)}$ of $C^{(i)*}$ is an ordinary double point of $C^{(i)*}$. We denote by $\sigma^*(C)$ the smallest integer N having the above property.

It is clear that $\sigma^*(C) = 0$ if and only if the origin P of C is an ordinary double point of C. If C is a regular curve then a strict interpretation of our definition of $\sigma^*(C)$ would require to set $\sigma^*(C) = 1$. However, we agree to set $\sigma^*(C) = 0$ also if C is a regular curve (this could also have been achieved by a slight change in our general definition of $\sigma^*(C))$. It is easily seen that $\sigma^*(C) = 1$ if and only if P is an ordinary s-fold point of C and $s > 2$.

Let C and D have the same number of branches and let $\pi : C \longrightarrow D$ be a pairing of the branches of C with the branches of D. If $\sigma^*(C) = 0$, i.e., if P is either a simple point or an ordinary double point of C, then we shall say that π is a (b)-equivalence between C and D if and only if also $\sigma^*(D) = 0$, i.e., if and only if the origin Q of D is a simple point or an ordinary double point of D according as P is a simple point or an ordinary double point of C. Assume that for all pairs Γ, $\triangle$ of algebroid curves, with the same number of branches, such that $\sigma^*(\Gamma) < \sigma^*(C)$, it has already been defined what is meant by saying that a pairing $\Gamma \longrightarrow \triangle$ between the branches of Γ and the branches of $\triangle$ is a (b)-equivalence. Then we define a (b)-equivalence between C and D as follows:

DEFINITION 2. A (b)-equivalence $\pi: C \longrightarrow D$ is a pairing π between the branches of C and the branches of D, having the following properties:

1) π is tangentially stable.

2) The pairings $\pi'_\nu : C'_\nu \longrightarrow D'_\nu$ $(\nu = 1, 2, \ldots, t)$ are (b)-equivalences.

3) If ε' and E' are the exceptional curves of the quadratic transformations T and S respectively (having centers at P

<u>and</u> Q), if $C'^{*}_{\nu} = C'^{*}_{\nu} \cup \mathcal{E}'$, $D'^{*}_{\nu} = D'_{\nu} \cup E'$, <u>and if</u> – <u>we extend the pairing</u> π'_{ν} <u>to a pairing</u> $\pi'^{*}_{\nu} : C'^{*}_{\nu} \longrightarrow D'^{*}_{\nu}$ <u>by</u> <u>setting</u> $\pi'^{*}_{\nu}(\mathcal{E}') = E'$, <u>then</u> π'^{*}_{ν} <u>is a</u> (b)-<u>equivalence</u>.

Note that conditions 1) and 2) of this definition are identical with the conditions 1) and 3) of Definition 1 ; condition 2) of Definition 1 has been deleted and has been replaced in Definition 2 by condition 3). Thus the equality of the multiplicities of corresponding branches under π is not explicitly postulated in Definition 2.

We now give a third definition of equivalence of algebroid singularities, which we shall refer to as <u>formal equivalence</u>. Again we proceed by induction on $\sigma^{*}(C)$, where we agree that if $\sigma^{*}(C) = 0$ formal equivalence coincides with (b)-equivalence.

DEFINITION 3. <u>Given two algebroid curves</u> C , D ,<u>having the same number of branches, we say that</u> C <u>and</u> D <u>are formally equivalent if there exists a tangentially stable pairing</u> $\pi : C \longrightarrow D$ <u>between the branches of</u> C <u>and the branches of</u> D <u>such that (in our previous notations)</u> :

1) C'_{ν} <u>and</u> D'_{ν} <u>are formally equivalent</u> ($\nu = 1, 2, \ldots, t$)
2) C'^{*}_{ν} <u>and</u> D'^{*}_{ν} <u>are formally equivalent</u> ($\nu = 1, 2, \ldots, t$) .

Note that this definition does not say anything about the nature of the pairings $\pi'_{\nu} : C'_{\nu} \longrightarrow D'_{\nu}$ and $\pi'^{*}_{\nu} : C'^{*}_{\nu} \longrightarrow D'^{*}_{\nu}$ induced by π .

Condition 1) merely requires that there exist, for each $\nu = 1, 2, \ldots, t$, some tangentially stable pairing $\rho'_\nu : C'_\nu \longrightarrow D'_\nu$ satisfying the conditions of the above inductive definition; and similarly, condition 2) requires that there exist a tangentially stable pairing $\rho'^*_\nu : C'^*_\nu \longrightarrow D'^*_\nu$ satisfying similar conditions. It is not even required that ρ'^*_ν be an extension of ρ'_ν. For this reason, Definition 3 is the most subtle (and also the weakest) of our three definitions of equivalence. The fact that these three definitions are all equivalent to each other is therefore not devoid of interest.

REMARK 1. In the case of characteristic $p \neq 0$ the following example poses the question of whether one should not attempt to look for a finer definition of equivalence in that case:

$$C : f = y^p + x^{2p+1} + ax^{2p-1}y = 0, \quad a \neq 0;$$
$$D : g = y^p + x^{2p+1} = 0.$$

It is easily seen that $C \equiv D$ in the sense of the preceding definitions. However, the module of derivations of the local ring of D is free (since $\frac{\partial g}{\partial y} = 0$), while the corresponding module for C is not free. Is such a qualitative difference between the two local rings compatible with a reasonable definition of equivalence?

REMARK 2. It is possible to generalize the definitions 1 and 2 to the case of a pair of arbitrary local rings of dimension 1, despite the fact that the numerical character similar to $\sigma(C)$ is not always available in the abstract case and that therefore the definition cannot be by induction. (It is known that it may not be possible to resolve a non-regular local ring of dimension 1 by successive quadratic transformations)

§3. <u>Analytic families of algebroid curves; equisingularity in codimension 1.</u>

Instead of attempting to establish an equivalence relation between two given singularities, one may try a less static and more fruitful approach, in which one considers an analytic family of singularities;

$$f(\{x\}; \{t\}) = 0, \tag{1}$$

where f is a power series in the coordinates $\{x\} = \{x_1, x_2, \ldots, x_{s+1}\}$ and the parameters $\{t\} = \{t_1, t_2, \ldots, t_\rho\}$, and where we assume that $f(\{0\}; \{t\})$ is identically zero. We have here a ρ-dimensional family of s-dimensional algebroid varieties W_t, embedded in an affine $(s+1)$-space and having a singular point at the origin $\{x\} = 0$. As one considers the specialization $\{t\} \longrightarrow \{0\}$, one may pose the following problem:

<u>Establish criteria which will give a meaning to the statement that the</u>

specialized variety W_0 has the same singularity at the origin as does the general member W_t of the family.

We can interpret equation (1) as defining an $(s + \rho)$ -dimensional embedded variety V, in the affine space of the $s + \rho + 1$ variables x and t. This variety V carries the irreducible subvariety $M : \{x\} = 0$, of dimension ρ (and codimension s). If we denote by P_t the general point $(\{0\}, \{t\})$ of M and by P_0 the special point $(\{0\}, \{0\})$ of M, then W_t is a section of V through P_t, transversal to M, and W_0 is a section of V through P_0, also transversal to M. Furthermore P_0 is a single point of M. One would not be far off the right track were one to say that the singularity of V at the general point P_t of M is the same as the singularity of V at the special point P_0 of M if and only if the transversal sections W_t and W_0 have equivalent singularities at P_t and P_0 respectively. We could therefore tentatively define equisingularity of an embedded variety V, along an irreducible subvariety M of V, at a simple point P_0 of M, as follows:

"DEFINITION "3. V is equisingular along M, at P_0, if there exists a section W_0 of V at P_0, transversal to M, and a section W_t of V at the general point P_t of M, also transversal to M, such that the singularity of W_0 at P_0 is equivalent to the singularity of W_t at P_t.

The trouble with this "definition" is that it is no definition at all, as long as we do not know what we mean by saying that W_0 and W_t have equivalent singularities. However, we can begin by testing this definition in the case in which the codimension s of M is equal to 1, in which case the trnasversal section are embedded algebroid curves, and for these we know what we mean by equivalent singularities. One obtains in this case a very satisfactory result at least in characteristic zero, via the following:

THEOREM 1. Let $f(x, y; \{t\}) = 0$ be an analytic family of plane algebroid curves C_t, all containing the origin $x = y = 0$, and defined over an algebraically closed ground field k of characteristic zero. Let $C_0 : f(x, y; \{0\}) = 0$ be the specialization of C_t for $\{t\} \longrightarrow 0$. Assume that f is regular in y, and let $\triangle^y f$ be the y-discriminant of f ($\triangle^y f \in k[[x, \{t\}]]$). Write $\triangle^y f = \mathcal{E}(x, \{t\}) x^N$, where $N \geqq 0$ and $\mathcal{E}(x, t) \in k[[x, \{t\}]]$ is such that $\mathcal{E}(0, \{t\}) \neq 0$. Then the following is true:

1) If $\mathcal{E}(0, \{C\}) \neq 0$, then C_t and C_0 are equivalent.

2) Conversely, if $C_t \equiv C_0$ and if the line $x = 0$ is not tangent to C_0, then $\mathcal{E}(0, \{0\}) \neq 0$.

3) More generally, if $C_t \equiv C_0$ and if the line $x = 0$ has the same intersection multiplicity with C_t and C_0, then $\mathcal{E}(0, \{0\}) \neq 0$.

We now interpret this theorem by looking at $f = 0$ as the equation of an algebroid embedded variety V of dimension $r = \rho + 1$, where ρ is, as above, the number of parameters t_i. The r elements $x, t_1, t_2, \ldots, t_\rho$ are parameters of the local ring of V at the point P_0. The equation $\Delta^y f = 0$, i.e., $\varepsilon(x, \{t\})x^N = 0$, is an equation of the critical variety Δ of the projection of V onto the affine space of the variables $x, t_1, t_2, \ldots, t_\rho$. To say that $\varepsilon(0, \{0\}) \neq 0$ means to say that Δ is the non-singular hypersurface $x = 0$ in that space. Note that Δ is then the projection of our subvariety M of V, of codimension 1, defined by $x = y = 0$. One then deduces from Theorem 1 the following:

THEOREM 2. *If* cod $M = 1$, *and* M *is part of the singular locus of* V, *then* V *is equisingular along* M *at* P_0, *if and only if there exist local parameters* $x_1, x_2, \ldots, x_r$ *of* V *at* P_0, *such that the critical variety* Δ *of the projection* π *of* V *onto the space of these parameters has a simple point at* $P'_0 = \pi(P_0)$. *Furthermore, if* V *is equisingular along* M *at* P_0, *and* $x_1, x_2, \ldots, x_r$ *are arbitrary transversal local parameters (by this we mean that the line* $x_1 = x_2 = \ldots = x_r = 0$ *is not tangent to* V *at* P_0), *then the corresponding ciritical variety* Δ *has necessarily a simple point at* P'_0.

At the Scientific conference at Yeshiva University last October, I spoke extensively about equisingularity in the case of codimension $s = 1$ and gave a number of other criteria of equisingularity in this case (always for characteristic zero). A limited number of copies of my Yeshiva lecture will be made available later on in informal discussions for those who are interested.

§4. Testing a general definition of equisingularity in a special case.

We maintain the assumption that the ground field k is algebraically closed and of characteristic zero. We consider again an r-dimensional algebroid variety V, embedded in an affine $(r + 1)$-space, an irreducible singular subvariety M of V, of codimension s on V, and a simple point P_0 of M. We shall define equisingularity of V at P_0, along M, by induction on s. If $x_1, x_2, \ldots, x_r$ are parameters of the local ring of V at P_0, we consider the projection π of V onto the affine r-space of the x_i, and we denote by Δ_x the corresponding critical hypersurface in that space. Then $\pi(M) \subset \Delta_x$, and $\pi(M)$ has codimension $s - 1$ on Δ_x.

DEFINITION 3. (Conjectural). V <u>is equisingular at the point</u> P_0 <u>along</u> M, <u>if there exist parameters</u> $x_1, \ldots, x_r$ <u>such that</u> Δ_x <u>is equisingular at the point</u> $\pi(P_0)$, <u>along</u> $\pi(M)$.

I have no general theory of equisingularity, based on this inductive definition. I will discuss this definition in a special, but theoretically important case.

There is one obvious and uncontestable case of equisingularity. That is the case in which V, as an algebroid variety, is locally, at P_0, a direct (analytic) product of M and a transversal section W_0, at P_0. That means that, for a suitable choice of the coordinates $x_1, x_2, \ldots, x_{r+1}$ in the ambient affine space of V, the equation of V involves only $s+1$ of the coordinates x_i, say

$$V: \; f(x_1, x_2, \ldots, x_{s+1}) = 0 ,$$

and M is the subvariety $x_1 = x_2 = \ldots = x_{s+1} = 0$. The transversal section W_0 at P_0 (the origin $x_1 = x_2 = \ldots = x_{r+1} = 0$) is given by the same equation $f = 0$, in the space of the $s+1$ coordinates $x_1, x_2, \ldots, x_{s+1}$. If σ and $\mathcal{O}$ denote respectively the local ring of V and W_0 at P_0, and if, for the sake of clarity, we denote the remaining coordinates $x_{s+2}, x_{s+3}, \ldots, x_{r+1}$ by $t_1, t_2, \ldots, t_\rho$ ($\rho = r - s$), then

$$\mathcal{O} = \sigma[[t_1, t_2, \ldots, t_\rho]] ,$$

and $t_1, t_2, \ldots, t_\rho$ are analytically independent over σ. We say in this case that V is <u>analytically equisingular at</u> P_0, <u>along</u> M.

Now, let us assume that the <u>critical variety</u> Δ_x (in Definition 3) <u>is analytically equisingular at the point</u> $\pi(P_0)$, <u>along the variety</u> $\pi(M)$.

Our variety V is then given by an equation

$$V : f(x_1, x_2, \ldots, x_s ; t_1, t_2, \ldots, t_\rho ; y) = 0 \quad (\rho = r - s),$$

where the power series f is regular in y ; the variety M is defined by $x_1 = x_2 = \ldots = x_s = y = 0$; and our assumption is that the y-discriminant $\Delta^y f$ of f is of the form

$$(2) \qquad \Delta^y f = \varepsilon(\{x\}, \{t\}), \; D(x_1, x_2, \ldots, x_s), \quad \varepsilon(\{0\}, \{0\}) \neq 0 .$$

Note that in the case of equisingularity in codimension $s = 1$, this assumption is automatically satisfied, for in that case we have, by Theorem 2: $\Delta^y f = \varepsilon(\{x\}, \{t\}) \, x_1^N$.

Another, theoretically important case in which this assumption is satisfied is the one in which the critical variety Δ_x has along $\pi(M)$ a normal crossing. Necessarily, we will have along $\pi(M)$ a normal crossing of s regular hypersurfaces, since $\operatorname{cod}_{\Delta_x} \pi(M) = s - 1$. That means that $\Delta^y f$ will be of the form (2), with $D = x_1^{N_1} x_2^{N_2} \ldots x_s^{N_s}$, $N_j \geqq 1$.

Under the above assumption (2), the following algebraic facts can be established:

Let $\mathcal{O}$ be the local ring of V at the point P_0 (the origin $\{x\} = \{t\} = y = 0$), and let σ be the local ring of the transversal section $W_0 : t_1 = t_2 = \ldots = t_\rho = 0$ at the same point P_0. Thus

$$(3) \qquad \mathcal{O} = k[[\{x\},\{t\}]][y] = k[[\{x\},\{t\},Y]]/(f(\{x\},\{t\},Y)) ,$$

and

$$(4) \qquad \sigma = k[[\{x\}]][\eta] = k[[\{x\},Y]]/(f_0(\{x\},Y)) ,$$

where

$$f_0(\{x\},Y) = f(\{x\},\{0\},Y) .$$

Let $\mathcal{O}'$ and σ' be the integral closure of $\mathcal{O}$ and σ respectively (in the total rings of quotients of these two local rings). Then

(a) <u>There is a natural injection of</u> σ' <u>into</u> $\mathcal{O}'$, <u>and</u> (<u>after identification</u> $\sigma' \subset \mathcal{O}'$) <u>it is true that the elements</u> $t_1, t_2, \ldots, t_\rho$ <u>of</u> $\mathcal{O}'$ <u>are analytically independent over</u> σ', <u>and</u> $\mathcal{O}'$ <u>is the power series ring</u> $\sigma'[[t_1, t_2, \ldots, t_\rho]]$.

By (a) we have for y a power series expansion of the form

$$(5) \qquad y = \eta + \sum u_i t_i + \sum u_{ij} \; t_i \; t_j + \ldots , \quad (u_i, u_{ij}, \ldots \in \sigma')$$

where η is the element which occurs in (4). Assumption (2) imposes, however, additional conditions on the coefficientss $u_i, u_{ij}, \ldots$ of the power series (5). We shall now state these conditions.

Since we have assumed that f_0 has no multiple factors, the total quotient ring K' of σ (= total quotient ring of σ') is a direct sum of fields $K_i' = K'e_i$ (say, $i = 1, 2, \ldots, h$), where $1 = e_1 + e_2 + \ldots + e_h$ is the decomposition of 1 into mutually orthogonal idempotents. Each field K_i' is an algebraic extension of the field Ke_i, where $K = k\{\{x\}\}$. We consider a fixed splitting field F' of the y-polynomial f_0, over K, and we embed each K_i' in F' by an isomorphism $K_i' \longrightarrow F_i$ which is an extension of the natural isomorphism $Ke_i \longrightarrow K$. Let $F'_i \supset F_i$ be the least Galois extension of K which contains F_i. Then F' is the composition of the h fields F_i' (the F_i' are splitting fields of the h irreducible factors of f_0).

Now, let ξ be any element of K'. For each $i = 1, 2, \ldots, h$, we denote by $\xi_i'^{(1)}, \xi_i'^{(2)}, \ldots, \xi_i'^{(n_i)}$ the conjugates, over K of the element of F_i which corresponds to ξe_i in the above embedding $K_i' \longrightarrow F_i$ of K_i' in F; here n_i is the relative degree of F_i over K. Let R be the set of elements ξ of $\mathfrak{o}'$ which have the following property: <u>For any</u> $i, j = 1, 2, \ldots, h$ <u>and any</u> $\alpha = 1, 2, \ldots, \eta_i$, $\beta = 1, 2, \ldots, \eta_j$, <u>the quotients</u>

$$(6) \qquad (\xi_i^{(\alpha)} - \xi_j^{(\beta)})/(\eta_i^{(\alpha)} - \eta_j^{(\beta)})$$

<u>are integral over</u> $k[[\{x\}]]$.

It is easily seen that R is a ring between $\mathfrak{o} = k[[\{x\}]][\eta]$ and $\mathfrak{o}'$.

Then we have

(b) *A necessary and sufficient condition that the discriminant* $\Delta^y f$ *be of the form* (2) *is that the coefficients* $u_i, u_{ij}, \dots$, *of the power series* (5) *belong to* R .

If our variety V was normal at P_0, then $\bar{\mathfrak{o}} = \bar{\mathfrak{o}}'$, $\mathfrak{o} = \mathfrak{o}'$, $\bar{\mathfrak{o}} = \mathfrak{o}[[t_1, t_2, \dots, t_\rho]]$, and we have in this case the trivial situation of analytical equisingularity of V along M, at P_0. But if V is not normal, then R will be in general a proper overring of $\bar{\mathfrak{o}}$, and if we choose the coefficients $u_i, u_{ij}, \dots$ in R, but not all in $\bar{\mathfrak{o}}$, then we get a situation of equisingularity which is not analytical. Thus this procedure gives us an effective tool for a general construction of an equisingularity phenomenon of the non-trivial (i.e., non analytic) type.

If we are in the complex domain then (6) and the fact that the coefficient of the power series (2) are all in R shows that

$$(7) \qquad \lim_{\{t\} \to 0} \frac{y^{(\alpha)} - y^{(\beta)}}{\eta^{(\alpha)} - \eta^{(\beta)}} = 1 ,$$

where the $y^{(\alpha)}$ are the roots of f and the $\eta^{(\alpha)}$ are the roots of $f^{(0)}$ ($\alpha, \beta = 1, 2, \dots, n = n_1 + n_2 + \dots + n_h$, $\alpha \neq \beta$).

By means of (7) it is possible to extend a proof given by Whitney in the case of codimension 1 and show that in the *ambient affine* $(r+1)$-*space* of V, the variety V can be isotopically deformed into the direct product of W_0 and M. This constitutes a fairly conclusive text of the correctness of the inductive definition 3 of equisingularity in this particular case.

On the structure of compact complex analytic surfaces

by K. Kodaira

By a <u>surface</u> we shall mean a compact complex manifold of complex dimension 2. We fix our notation as follows.

S: a surface

b_ν: the ν-th Betti number of S,

c_ν: the ν-th Chern class of S,

$\mathcal{O}$: the sheaf over S of germs of holomorphic functions,

$q = \dim H^1(S, \mathcal{O})$: the irregularity of S,

$P_g = \dim H^2(S, \mathcal{O})$: the geometric genus of S.

Note that c_1^2 and c_2 are (rational) integers.

By a theorem of Grauert [2], any surface is obtained from a surface containing no exceptional curve (of the first kind) by means of a finite number of quadric transformations. Hence, in order to study the structure of surfaces, it suffices to consider surfaces containing no exceptional curves. In what follows we assume that all surfaces under consideration contain no exceptional curves.

DEFINITION 1. By an elliptic surface we shall mean a surface S with a holomorphic map ψ of S onto a non-singular algebraic curve Δ such that the inverse image $\psi^{-1}(u)$ of any general point

$u \in \Delta$ is an elliptic curve. We call Δ the base curve of the elliptic surface S.

DEFINITION 2. (A. Weil). We call a surface S a K3 surface if S is a deformation of a non-singular quartic surface in a projective 3-space. e.g. $z_0^4 + z_1^4 + z_2^4 + z_3^4 = 0$

MAIN THEOREM. Surfaces (containing no exeptional curves) can be classified into the following seven classes :

I) the class of algebraic surfaces with $p_g = 0$;

II) the class of K3 surfaces;

III) the class of complex tori (of complex dimension 2) ;

IV) the class of elliptic surfaces with $b_1 \equiv 0(2)$, $p_g \geqq 1$, $c_1 \neq 0$;

V) the class of algebraic surfaces with $p_g \geqq 1$, $c_1^2 > 0$;

VI) the class of elliptic surfaces with $b_1 \equiv 0(1)$, $p_g \geqq 1$;

VII) the class of surfaces with $b_1 = q = 1$, $p_g = 0$.

class	b_1	p_g	c_1	c_1^2	structure
I	even	0			algebraic
II	0	1	=0	0	K3 surfaces
III	4	1	=0	0	complex tori
IV	even	+	≠0	0	elliptic
V	even	+		+	algebraic
VI	odd	+		0	elliptic
VII	1	0			?

An elliptic surface is a deformation of an algebraic surface if and only if its first Betti number is even (see [4]) . Therefore the following theorem follows from the main theorem.

THEOREM . A surface is a deformation of an algebraic surface if and only if its first Betti number is even.

Remark: The class VII contains many elliptic surfaces. In fact,
$H_1 = \mathbb{Z} \oplus A$
for any preassigned finite abelian group A , we find an elliptic surface of the class VII whose first torsion group is isomorphic to A . We obtain examples of non-elliptic surfaces of the class VII as follows : Let $\mathbb{C}^2$ denote the space of two complex variables (z_1, z_2) and let $U = \mathbb{C}^2 - (0,0)$. Choose a properly discontinuous group $\mathcal{G}$ of analytic automorphisms without fixed points of U in an appropriate manner. Then the quotient surface $S = U/\mathcal{G}$ is a non-elliptic surface of the class VII. Note that $S = U/\mathcal{G}$ is a deformation of an elliptic surface. As far as we know there is no example of a surface which cannot be deformed into surfaces with non-constant meromorphic functions.

We shall outline a proof of the main theorem. Let $\mathcal{O}^*$ be the multiplicative sheaf over S of germs of non-vanishing holomorphic functions and let $\mathbb{Z}$ denote the ring of rational integers. We have the exact sequence

$$(1) \qquad \cdots \to H^1(S, \mathcal{O}) \to H^1(S, \mathcal{O}^*) \xrightarrow{\delta^*} H^2(S, \mathbb{Z}) \to H^2(S, \mathcal{O}) \to \cdots$$

Each element F of $H^1(S, \mathcal{O}^*)$ represents a complex line bundle over S and $c(F) = \delta^* F$ is the Chern class of F. Let $\mathcal{O}(F)$ denote the sheaf over S of germs of holomorphic sections of F. In the case of complex line bundles over surfaces, the Riemann-Roch-Hirzebruch theorem can be formulated as follows :

$$(2) \qquad \sum_{\nu=0}^{2} (-1)^\nu \dim H^\nu(S, \mathcal{O}(F)) = \frac{1}{2}(c^2 + c_1 c) + \frac{1}{12}(c_1{}^2 + c_2), \qquad c = c(F)$$

(see Atiyah and Singer [1]). This theorem implies the Noether formula

$$(3) \qquad 12(p_g - q + 1) = c_1{}^2 + c_2$$

and the Riemann-Roch inequality

$$(4) \qquad \dim H^0(S, \mathcal{O}(F)) + \dim H^0(S, \mathcal{O}(K-F)) \geqq \frac{1}{2}(c^2 + c_1 c) + p_g - q + 1 ,$$

where K denotes the canonical bundle of S.

THEOREM 1. Every holomorphic 1-form on a surface is d-closed.

THEOREM 2. Let $\varphi_1, \varphi_2, \ldots, \varphi_n$ be holomorphic 1-forms on S. If $\varphi_1, \ldots, \varphi_n$ are linearly independent, then the d-closed 1-forms $\varphi_1, \ldots, \varphi_n, \bar{\varphi}_1, \ldots, \bar{\varphi}_n$ are d-cohomologically independent.

Letting $\{ \Gamma_1, \ldots, \Gamma_j, \ldots, \Gamma_{b_2} \}$ be a Betti base of 2-cycles on S and denoting by $I(\Gamma_j, \Gamma_k)$ the intersection multiplicity of Γ_j

and Γ_k, we define b^+ and b^- to be respectively the number of positive and negative eigenvalues of the non-singular symmetric matrix $(I(\Gamma_j, \Gamma_k))$. Moreover we denote by h the number of linearly independent holomorphic 1-forms on S. With the aid of Theorems 1 and 2, we obtain from the Hirzebruch index theorem and the Noether formula (3) the equality

$$2q - b_1 + b^+ - 2p_g = 1,$$

while we have the inequalities

$$q \geqq \frac{1}{2} b_1 \geqq h \geqq b_1 - q, \qquad b^+ \geqq 2p_g \quad .$$

Hence we obtain the following

THEOREM 3. If b_1 is even, then $b_1 = 2q$, $b^+ = 2p_g + 1$ and $h = q$. If b_1 is odd, then $b_1 = 2q - 1$, $b^+ = 2p_g$ and $h = q - 1$.

COROLLARY. We have the formula

$$(5) \qquad c_1^{\,2} + 8q + b^- = \begin{cases} 10p_g + 9, & \text{if } b_1 \text{ is even}, \\ 10p_g + 8, & \text{if } b_1 \text{ is odd}. \end{cases}$$

Let us consider the case in which b_1 is even. By the above results there exist q linearly independent d-closed holomorphic

1-forms $\varphi_1, \varphi_2, \dots, \varphi_q$ on S. Let $\{\gamma_1, \dots, \gamma_j, \dots, \gamma_{2q}\}$ be a Betti base of 1-cycles on S and let

$$\omega_{\nu j} = \int_{\gamma_j} \varphi_\nu \quad .$$

Then, by Theorem 2, the vectors

$$\omega_j = (\omega_{1j}, \dots, \omega_{\nu j}, \dots, \omega_{qj}) , \qquad j = 1, 2, \dots, 2q .$$

are linearly independent with respect to real coefficients and generate a discontinuous subgroup $\mathcal{D}$ of the vector group $\mathbb{C}^q$ of dimension q. We call $\mathcal{A} = \mathbb{C}^q/\mathcal{D}$ the Albanese variety attached to S and define a holomorphic map Φ of S into $\mathcal{A}$ in an obvious manner.

THEOREM 4. If there exist on S two algebraically independent meromorphic functions, then S is an algebraic surface. If there exists on S one and only one algebraically independent meromorphic function, then S is an elliptic surface (see [3]).

The following three theorems follow immediately from this theorem.

THEOREM 5. If there exists on S a complex line bundle F such that $\dim H^0(S, \mathcal{O}(F)) \geqq 2$, then S is either an algebraic surface or an elliptic surface.

THEOREM 6. If $p_g \geqq 2$, then S is either an algebraic surface or an elliptic surface.

THEOREM 7. If $h \geqq 3$, then S is either an algebraic surface or an elliptic surface.

Combining the Riemann-Roch inequality (4) with Theorem 5, we obtain the following two theorems.

THEOREM 8. If there exists on S a complex line bundle F with $c(F)^2 > 0$, then S is an algebraic surface.

THEOREM 9. If $c_1^2 > 0$, then S is an algebraic surface.

THEOREM 10. If b_1 is even and if $p_g = 0$, then S is an algebraic surface.

Proof: Since, by Theorem 3, $b^+ = 1$, there exists an element $c \in H^2(S, \mathbb{Z})$ with $c^2 > 0$. Moreover, since $H^2(S, \mathcal{O})$ vanishes, the exact sequence (1) shows the existence of a complex line bundle F over S with $c(F) = c$. Hence, by Theorem 8, S is an algebraic surface.

LEMMA 1. If $p_g \geqq 1$, then $c_1^2 \geqq 0$.

THEOREM 11. Assume that there exists on S no meromorphic function except constants (and that S contains no exceptional curve). Then the irregularity q of S is not greater than 2. If $q = 2$, then S is a complex torus. If $q = 1$, then the first Betti number b_1 of S is equal to 1 and the geometric genus p_g of S vanishes. If $q = 0$, then the first Chern class c_1 of S vanishes.

Proof: A) The case in which b_1 is even. It follows from Theorems 3, 6, 7 and 10 that $b_1 = 2q$, $q = h \leqq 2$ and $p_g = 1$. Hence, by Lemma 1 and Theorem 9, $c_1{}^2 = 0$.

i) q is equal to either 2 or 0. In fact, if q were equal to 1, then the Albanese variety $\mathscr{A}$ would be an elliptic curve and the meromorphic functions on $\mathscr{A}$ would induce non-constant meromorphic functions on S.

ii) If $q = 2$, then the Albanese variety $\mathscr{A}$ is a complex torus and Φ maps S biholomorphically onto $\mathscr{A}$.

iii) If $q = 0$, then we have

$$\dim H^0(S, \mathcal{O}(-K)) + \dim H^0(S, \mathcal{O}(2K)) \geqq 2 .$$

Hence, in view of Theorem 5, $\dim H^0(S, \mathcal{O}(-K)) = 1$, while $\dim H^0(S, \mathcal{O}(K)) = p_g = 1$. Consequently K is trivial and c_1 vanishes.

B) The case in which b_1 is odd. It follows from Theorems 3, 6, 7 and 9 that $b_1 = 2q - 1$, $q = h + 1$, $b^+ = 2p_g$, $h \leqq 2$, $p_g \leqq 1$ and $c_1^2 \leqq 0$.

i) Suppose that $h = 2$. Then there exist on S two linearly independent holomorphic 1-forms φ_1 and φ_2 and $\varphi_1 \wedge \varphi_2$ does not vanish identically. Hence $p_g = 1$ and, by Lemma 1, $c_1^2 = 0$. The formula (5) then proves that $b^- = -6$. This is a contradiction.

ii) Suppose that $h = 1$. We take a d-closed holomorphic 1-form φ on S and find a 1-form σ of type $(1,0)$ on S such that $d\sigma = \varphi \wedge \bar{\varphi}$ and such that $\sigma + \bar{\sigma}$, φ and $\bar{\varphi}$ generate the d-cohomology group of 1-forms on S. We then obtain multi-valued holomorphic functions w_1 and w_2 on S such that

$$dw_1 = \varphi, \quad dw_2 = \sigma + \bar{w}_1 \varphi.$$

The exterior product $dw_1 \wedge dw_2$ does not vanish at each point of S. Hence the space $\mathbb{C}^2$ of the complex variables w_1 and w_2 forms the universal covering surface of S. The covering transformation group of $\mathbb{C}^2$ over S is generated by the affine transformations

$$g_j : w_1 \longrightarrow w_1 + \alpha_j, \quad w_2 \longrightarrow w_2 + \bar{\alpha}_j w_1 + \beta_j, \quad j = 1, 2, 3, 4.$$

of which the coefficients satisfy the conditions that

$$\alpha_4 = 0, \; \bar{\alpha}_j \alpha_k - \bar{\alpha}_k \alpha_j = n_{jk} \beta_4, \qquad \text{for } j, k = 1, 2, 3,$$

where the n_{jk} are integers and $n_{23}\beta_4 \neq 0$. It follows that S is an elliptic surface. This contradicts the non-existence of meromorphic functions on S.

iii) Thus we see that $h = 0$ and $q = b_1 = 1$. Therefore the Picard variety $\mathcal{P} = H^1(S,\mathcal{O})/H^1(S, \mathbb{Z})$ is isomorphic to the Lie group $\mathbb{C}/\mathbb{Z}$. Suppose that $p_g = 1$. Then, for __each__ complex line bundle $F \in \mathcal{P}$, the inequality

$$\dim H^0(S,\mathcal{O}(F)) + \dim H^0(S,\mathcal{O}(K-F)) \geqq 1$$

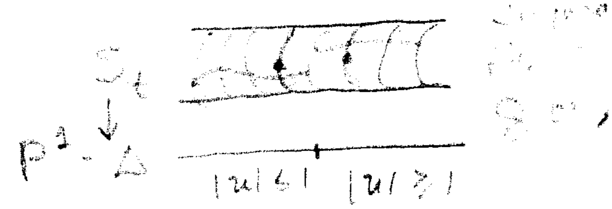
holds. It follows that there exist infinitely many irreducible curves on S. This contradicts the non-existence of meromorphic function on S (see [3]), q.e.d.

THEOREM 12. If the irregularity q and the first Chern class c_1 of S both vanish, then S is a K3 surface.

__Proof:__ Denoting by Θ the sheaf over S of germs of holomorphic vector fields, we have

$$\dim H^1(S, \Theta) = 20, \quad \dim H^2(S, \Theta) = 0.$$

Hence there exists a complete complex analytic family of small deformations S_t of S depending on 20 effective parameters $(t_1, t_2, \ldots, t_{20})$ (see Kodaira, Nirenberg and Spencer [5]). We find



t such that S_t is a non-algebraic elliptic surface of which the singular fibres are either of type I_1, or of type II (compare [3]). S_t is a fibre preserving deformation of an algebraic elliptic surface B which possesses a global holomorphic section. B can be described explicitly as follows : Let $\mathbb{P}^2$ denote a projective plane on which a system of homogeneous coordinates (c, y, z) is fixed. Take two copies $\mathbb{P}^2 \times \mathbb{C}_0$ and $\mathbb{P}^2 \times \mathbb{C}_1$ of $\mathbb{P}^2 \times \mathbb{C}$ and form their union

$$W = \mathbb{P}^2 \times \mathbb{C}_0 \cup \mathbb{P}^2 \times \mathbb{C}_1$$

by identifying $(x, y, z, u) \in \mathbb{P}^2 \times \mathbb{C}_0$ with $(x_1, y_1, z_1, u_1) \in \mathbb{P}^2 \times \mathbb{C}_1$ if and only if $uu_1 = 1$, $u^4 x_1 = x$, $u^6 y_1 = y$, $z_1 = z$. Then B is the subvariety of W defined by an equation of the form

$$y^2 z - 4x^3 + \tau_0 x z^2 \prod_{\nu=1}^{8} (u - \tau_\nu) + z^3 \prod_{\nu=1}^{12} (u - \sigma_\nu) = 0 .$$

To make explicit the dependence of B on the coefficients $\tau = (\tau_0, \tau_1, \ldots, \tau_8, \sigma_1, \ldots, \sigma_{12})$, we write B_τ for B. Clearly B_τ is a deformation of $B^0 = B_{(1, \ldots, 1, 0, \ldots, 0)}$. Hence S is a deformation of B^0. Let Q denote a non-singular quartic surface in a projective 3-space. The irregularity and the first Chern class of Q both vanish. Hence, by the above result, Q is a deformation of B^0 and, consequently, S is a deformation of Q. Thus we see that S is a K3 surface.

THEOREM 13. If the canonical bundle K of S is trivial, then S is a $K3$ surface, a complex torus, or an elliptic surface of the form $\mathbb{C}^2/G$, where G is a properly discontinuous group of affine transformations without fixed points of the space $\mathbb{C}^2$ of two complex variables z_1, z_2 which leave invariant the 2-form $dz_1 \wedge dz_2$. The first Betti number of the elliptic surface $\mathbb{C}^2/G$ is equal to 3.

LEMMA 2. If b_1 is even, $p_g > 0$ and $c_1 = 0$, then the canonical bundle K of S is trivial.

LEMMA 3. If p_g is positive, $c_1^2 = 0$ and $c_1 \neq 0$, then S is an elliptic surface.

Now, with the aid of Lemmas 1, 2, 3, we derive readily from Theorems 9-13 the main theorem.

References

[1] M. F. Atiyah and I. M. Singer, "The index of elliptic operators on compact manifolds", Bull. Amer. Math. Soc., 69 (1963), pp. 422-433 .

[2] H. Grauert, "Über Modifikationen und exzeptionelle analytische Mengen", Math. Ann., 146 (1962), pp. 331-368 .

[3] K. Kodaira, "On compact complex analytic surfaces, I", Annals of Math., 71 (1960), pp. 111-152 .

[4] K. Kodaira, "On compact analytic surfaces, II-III", Annals of Math., 77 (1963), pp. 563-626, 78 (1963), pp. 1-40 .

[5] K. Kodaira, L. Nirenberg and D. C. Spencer, "On the existence of deformations of complex analytic structures", Annals of Math., 68 (1958), pp. 450-459 .

ON DEFORMATIONS AND VARIETIES OF MODULI

T. Matsusaka

§1. The notion of polarization is well-known by now. But we shall start with this definition. Let V be a complete non-singular algebraic variety and $G_a(V)$ the group of V-divisors which are algebraically equivalent to zero. Denote by $T(V)$ the group of torsion divisors on V and by $t(V)$ the order of $T(V)$. We consider a set $\mathfrak{X}$ of V-divisors which is defined by the following conditions:

(a) $\mathfrak{X}$ contains a divisor x on X which is non-degenerate (ample in the sense of Grothendieck);

(b) A V-divisor Y is in $\mathfrak{X}$ if and only if there is a pair (r, s) of integers which are relatively prime to the characteristic p and to $t(V)$ such that $rX \equiv sY \mod G_a(X)$.

We consider that the set $\mathfrak{X}$ defines a structure on V. V, together with this additional structure, is denoted by $\underline{V}$ and is called a *polarized variety*. We call V the *underlying variety* of $\underline{V}$ and $\mathfrak{X}$ the *structure set* of $\underline{V}$. A divisor in $\mathfrak{X}$ is called a *polar divisor* of $\underline{V}$.

REMARK. If one wants to deal with a variety over a discrete valuation ring, of which V is a generic fibre, it is convenient to take p to be the characteristic of the residue field.

Basically, we shall follow the terminology and conventions of Weil's "Foundations of Algebraic Geometry".

PROPOSITION 1. Let $\underline{V}$ be a polarized variety. Then there is a polar divisor X_o with the following properties: (i) A V-divisor Y is a polar divisor of $\underline{V}$ if and only if it is algebraically equivalent to mX_o where m is an integer; (ii) A non-degenerate polar divisor on $\underline{V}$ is algebraically equivalent to mX_o where m is a positive integer. Moreover, the class of X_o mod $G_a(V)$ is uniquely determined by these conditions.

X_o is called a basic polar divisor of $\underline{V}$. The self-intersection number of X_o is called the <u>rank</u> or the <u>degree</u> of $\underline{V}$. A non-singular subvariety of a projective space can have a natural polarization such that a hyperplane section is a polar divisor. We call it a <u>natural polarization</u> and all such varieties shall be assumed to carry their natural polarization.

Let U be a complete (proper) abstract variety over a discrete valuation ring $\mathfrak{o}$, α the canonical morphism of U onto $\mathfrak{o}$ and $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$. Then $\alpha^{-1}(\mathfrak{p})$ is called the <u>specialization</u> of $\alpha^{-1}(0)$ over $\mathfrak{o}$. If X is a cycle on a generic fibre $\alpha^{-1}(0)$, rational over the quotient field k of $\mathfrak{o}$, it defines a U-cycle $\widetilde{X}$ uniquely such that $\widetilde{X} \cdot \alpha^{-1}(0) = X$, and that every component of $\widetilde{X} \cap \alpha^{-1}(\mathfrak{p})$ which is simple on U is proper. Then $\widetilde{X} \cdot \alpha^{-1}(\mathfrak{p})$ is called the specilization of X over $\mathfrak{o}$. $\widetilde{X} \cdot \alpha^{-1}(\mathfrak{p})$ is still the specilization of X over a discrete valuation ring which dominates $\mathfrak{o}$.

Let $\underline{V}$ be a polarized variety, V its underlying variety and k a field of definition of $\underline{V}$. Let $\mathfrak{o}$ be a discrete valuation ring of k, U the variety over $\mathfrak{o}$ with the canonical morphism α whose generic fibre is V and W the special fibre $\alpha^{-1}(\mathfrak{p})$ of U. Assume that W is the underlying variety of a polarized variety $\underline{W}$ and that a basic polar divisor X_0 of $\underline{V}$ specializes to a polar divisor of $\underline{W}$ over $\mathfrak{o}$. Then we say that $\underline{W}$ is the <u>specialization</u> of $\underline{V}$ over $\mathfrak{o}$ and write

$\underline{V} \longrightarrow \underline{W}$ ref. $\mathfrak{o}$.

REMARK. When $\underline{V} \longrightarrow \underline{W}$ ref. $\mathfrak{o}$, then rank (V) $\geq$ rank ($\underline{W}$). When $\mathfrak{o}$ contains the rational number field, we have rank ($\underline{V}$) = rank ($\underline{W}$) because of Hodge's theorem. On the other hand, when the quotient field of $\mathfrak{o}$ is of characteristic p, Nishi constructed an example such that rank ($\underline{V}$) > rank ($\underline{W}$). In his example, $\underline{W}$ is a suitably polarized Abelian variety of dimension 2 and one can choose $\underline{V}$ so that rank ($\underline{V}$) exceeds a given positive integer.

In general, the concept of specialization is not invariantly attached to isomorphism classes of polarized varieties. However we have the following result.

PROPOSITION 2. Let $\underline{V}$, $\underline{V}'$, $\underline{W}$, $\underline{W}'$ be four polarized varieties, k a common field of definition of $\underline{V}$ and $\underline{V}'$, $\mathfrak{o}$ a discrete valuation ring of k and assume that $(\underline{V}, \underline{V}') \longrightarrow (\underline{W}, \underline{W}')$ ref. $\mathfrak{o}$. When there is an isomorphism f of $\underline{V}$ to $\underline{V}'$ defined over k and when $\underline{W}'$ is not ruled, the graph of f specializes to the graph of an isomorphism between $\underline{W}$ and $\underline{W}'$ over $\mathfrak{o}$.

Let now $\underline{V}$ and $\underline{W}$ be two polarized varieties and the $\underline{V}_i$, for $0 \leq i \leq$ $\underline{V}_0 = \underline{V}$, , $\underline{V}_m = \underline{W}$, be a finite set of polarized varieties. Assume that either $\underline{V}_i$ and $\underline{V}_{i+1}$ are isomorphic to each other, or the one is a specialization of the other over some discrete valuation ring. Then we say that $\underline{W}$ is a <u>defermation</u> of $\underline{V}$, $\underline{V}$ is a <u>deformation</u> of $\underline{W}$ or $\underline{V}$ and $\underline{W}$ are <u>deformations</u> of each other. If rank $(\underline{V}_i) \leq$ d for all i, we say that the deformation is of <u>type</u> d. Denote by Σ the set of deformations of a given polarized variety $\underline{V}$. Denote also by Σ_d the set of deformations of $\underline{V}$ of type d for $d \geq$ rank $(\underline{V})$. In the case of characteristic 0, we have $\Sigma = \Sigma_d$. Therefore, we shall consider only Σ_d from now on. We introduce an equivalence relation $\sim$ in Σ_d. We say that $\underline{U}$ and $\underline{W}$ in Σ_d are equivalent and write $\underline{U} \sim \underline{W}$ if and only if $\underline{U}$ and $\underline{W}$ are isomorphic. The quotient space of Σ_d by this equivalence relation will be called the <u>space of moduli</u> and denoted by $\mathfrak{M}$. Our basic problem is to find out the structure of this space. One is tempted to say that it is an algebraic variety, or at least a finite union of such varieties. Furthermore, one is tempted to say that the largest dimension of the maximal component can be described in terms of numerical invariants of $\underline{V}$ (cf. works of Kodaira-Spencer). As it is well-known, these are true when one deals with curves or polarized Abelain varieties (cf. works of Baily, Mumford). In general Σ_d can be expressed as a union of countably many irreducible algebraic families of polarized varieties up to isomorphisms In order to pursue our problems further, we introduce the concept of a universal family.

Let $\mathcal{F}$ be an algebraic family, i.e. a union of a finite set of irreducible algebraic families, of non-singular varieties in a projective space such that

(i) A member of $\mathcal{F}$ is a member of Σ_d ;

(ii) A member of Σ_d is isomorphic to a member of $\mathcal{F}$.

Then we say that $\mathcal{F}$ is a <u>universal family</u> of Σ_d. The universal family of Σ_d exists if and only if the following is true.

<u>There is a constant</u> c, <u>depending only on</u> Σ_d, <u>such that whenever</u> <u>W</u> <u>is a member of</u> Σ_d <u>and</u> Y <u>a basic polar divisor of</u> <u>W</u>, mY <u>is ample</u> (very ample in the sense of Grothendieck) <u>for</u> $m > c$.

Of course, this conjecture is true when <u>V</u> is a curve or a polarized Abelian variety. When <u>V</u> is a polarized surface, this conjecture is affirmative and can be deduced from the following theorem.

THEOREM 1. Let V be a non-singular complete surface and X a non-degenerate V-divisor. Let $|p_a(X)| < c_1$, $X^{(2)} < c_2$ and $|p_a(V)| < c_3$. Then, there is a constant, depending only on c_1, c_2, c_3, such that mX is ample for $m > c$.

When the dimension of <u>V</u> is higher than 2, nothing is known in general. Kim showed that if <u>V</u> can be mapped into Albanese variety without fundamental subvarieties, the subset of Σ_d consisting of polarized varieties with the same property has a universal family. Assuming only that $\underline{V}$ can be mapped into its Albanese variety without decreasing its dimension, we can show now that Σ_d has a universal family.

A weaker problem than the existence of a universal family, which seems to be worthwhile to solve nevertheless, is the following. Let X be an ample polar divisor of $\underline{V}$, f_1 a non-degenerate projective embedding of $\underline{V}$ determined by X and $\mathcal{F}_1$ a maximal algebraic family of non-singular prpjective varieties such that each component $\mathcal{F}_1$ contains $f_1(\underline{V})$. Let $\mathcal{M}_1$ be the quotient space of $\mathcal{F}_1$ which we get by identifying members of $\mathcal{F}_1$ which are isomorphic to each other. Let $X_2 = m_2 X$, where m_2 is a positive integer, and define f_2, $\mathcal{F}_2$, $\mathcal{M}_2$ as f_1, $\mathcal{F}_1$, $\mathcal{M}_1$. When we continue this process, we get a sequence of quotient spaces $\{\mathcal{M}_i\}$ and morphisms $g_i : \mathcal{M}_1 \longrightarrow \mathcal{M}_{i+1}$. One can introduce the quotient topology on $\mathcal{M}_i$ and g_i becomes an injection with respect to this topology. Then one can show that there is an open subset $\mathcal{M}'_i$ on each $\mathcal{M}_i$, which is everywhere dense in $\mathcal{M}_i$, such that it has a structure of a union of a finite set of irreducible algebraic varieties. Moreover, g_i induces on each $\mathcal{M}'_i$ a birational morphism such that the closure of the image is $\mathcal{M}_{i+1}$. Then, one could ask if there is a constant c such that g_i is a bijection when $i > c$. When the answer to this is affirmative, we shall call

$\mathcal{F}_m$, for $m > c$, a <u>local universal family at $\underline{V}$</u>.

Once the question of the existence of a universal family of Σ_d, or at least the existence of a local universal family at $\underline{V}$ is settled affirmatively, the study of the space of moduli $\mathcal{M}$ (resp. local space of moduli) can be reduced to the study of the quotient space of the universal family (resp. local universal family). But the problem of studying a quotient space of an algebraic variety with respect to an equivalence relation is not a trivial problem. For this purpose, we have to analyze our equivalence relation on a universal family (resp. local universal family) more closely.

THEOREM 2. Let us assume that a universal family of Σ_d (resp. local universal family at $\underline{V}$) exists. Then there exists a universal family (resp. local universal family) $\mathcal{F}$ with the following properties:

(i) $\mathcal{F}$ is a union of a finite set of irreducible maximal algebraic families $\mathcal{F}_i$ in a projective space;

(ii) When $\underline{U}$ is in $\mathcal{F}_i$ and $\underline{W}$ is in $\mathcal{F}$ such that $\underline{U} \sim \underline{W}$, then $\underline{W}$ is in $\mathcal{F}_i$;

(iii) Let Y be a $\underline{U}$-divisor which is algebraically equivalent to a hyperplane section of $\underline{U}$ and call $\mathcal{L}(Y)$ the corresponding invertible sheaf on $\underline{U}$. Then $h^i(\mathcal{L}(Y)) = 0$ for $i > 0$ whenever $\underline{U} \in \mathcal{F}$.

From now on, we shall consider only those universal families (resp. local universal families) which satisfy (i), (ii), (iii) of the above theorem. When that is so, the study of the quotient space of $\mathcal{F}$ can be reduced substantially to those of $\mathcal{F}_i$. In order to do so, we shall assume that Σ_d does not contain a ruled variety. Let F_i be the Chow-variety of $\mathcal{F}_i$ and denote by $0(x)$ the orbit of $x \in F_i$ with respect to our equivalence relation. Then our equivalence relation satisfies the following conditions.

THEOREM 3. (I) The equivalence relation on F_i is a closed equivalence relation; (II) $0(x)$ is an irreducible and locally closed subvariety of F_i; (III) Let k be a field of definition of F_i, x a point of F_i and x' a point of F_i such that $x \longrightarrow x'$ ref. k. Identifying $0(x)$, $0(x')$ with cycles in the ambient projective space, we have $0(x) \longrightarrow m0(x')$ ref. k, where m is a positive integer.

REMARK. Actually, m can be described in terms of the relative change of groups of automorphisms of members of $\mathcal{F}_i$, but we are not going into the detail of this fact.

§2. Nagata has constructed an example of a non-singular locally closed subvariety of a projective space, carrying an equivalence relation which satisfies (I), (II), (III) of Theorem 3, such that the quotient space is not an algebraic variety. On the other hand, we encounter quite often an equivalence relation of this type on an algebraic variety in algebraic geometry. (perhaps omitting the condition that $0(x)$ is irreducible). Moreover, even if the quotient space is an algebraic variety and F_i is non-singular, it cannot be non-singular in general. Therefore, it seems to be desirable to have some theory which eliminates these difficulties. For this reason, we shall introduce the concept of Q-varieties and Q-manifolds, which can be described briefly as follows.

Let V be an algebraic variety defined over a field k and $\bar{\Gamma}$ a k-closed subset of $V \times V$. When P is a point of V, define $\bar{\Gamma}\{P\}$ by $P \times V \cap \bar{\Gamma} = P \times \bar{\Gamma}\{P\}$. Assume that $(V, \bar{\Gamma})$ has the following properties. $\bar{\Gamma} = \bigcup \Gamma_i$ Γ_i irred.

(a) Every component Γ_i of $\bar{\Gamma}$ has the geometric projection V on each factor of the product $V \times V$; $0 \leftarrow V \leftarrow \Gamma_i \rightarrow V \rightarrow 0$, $\dim \Gamma_i = \dim \Gamma_j$

(b) $\bar{\Gamma}$ defines an equivalence relation on V; i.e. $P \sim Q \Leftrightarrow P \times Q \in \bar{\Gamma}$

(c) When P and P' are points on V such that P' is a specialization of P over k, $\bar{\Gamma}\{P'\}$ is a uniquely determined specialization of $\bar{\Gamma}\{P\}$ over k over the specialization $P \longrightarrow P'$ ref. k;

(d) When P is a generic point of V over k, every component of $\bar{\Gamma}\{P\}$ is separably algebraic over $k(P)$.

It can be verified easily, using Theorem 3, that the equivalence relation on F_i satisfies these four conditions.

Let $\mathcal{V}$ be a quotient space of V by this equivalence relation and φ the canonical map of V on $\mathcal{V}$. We make $\mathcal{V}$ a topological space by taking the quotient topology and calling it a Q-<u>variety</u>. Let k be a field of definition of V such that $\Gamma = \sum \Gamma_i$ is rational over it. k is then called a field of definition of $\mathcal{V}$. When P is a point of V, $\varphi(P)$ is called a point of $\mathcal{V}$. When P' is another point of V such that P' is a specialization of P over k, we say that $\varphi(P')$ is a specialization of $\varphi(P)$ over k. Next, assume that $\bar{\Gamma}\{P\}$ contains a simple point Q on V and set $(Q \times V) . \Gamma = Q \times \Gamma(Q)$. $\Gamma(Q)$ is then uniquely determined by $\bar{\Gamma}\{P\}$, i.e., by $\varphi(P)$. Hence we denote it by $\Gamma(\varphi(P))$. Let $\Gamma(\varphi(P)) = \sum a_i X_i + \sum b_j Y_j$ be the reduced expression for $\Gamma(\varphi(P))$ such that $a_i \not\equiv 0(p)$ and $b_j \equiv 0(p)$. Denote $\sum a_i X_i$ by $\Gamma(\varphi(P))_0$ and $\sum b_j Y_j$ by $\Gamma(\varphi(P))_p$. We call $\varphi(P)$ a <u>regular point</u> of $\mathcal{V}$, and a p-<u>regular point</u> if $\Gamma(\varphi(P))_0 \neq 0$. If $\varphi(P)$ is a p-regular point of $\mathcal{V}$, $\Gamma(P)_0$ has a smallest field K, containing k, over which it is rational. Denote K by $k(\varphi(P))$. It can be shown that this field is also a smallest field, containing k, over which $\Gamma(\varphi(P))$ is rational. If $\varphi(P)$ is not a p-regular point on $\mathcal{V}$, set $\bar{\Gamma}\{P\} = \cup Z_i$ and $Z = \sum Z_i$. Z has a smallest field K', containing k, over which it is rational. We denote K' by $k(\varphi(P))$.

REMARK. When $\varphi(P)$ is p-regular, we could associate K' over k by means of the latter method. It can be shown that K' contains $k(\varphi(P))$ and that the former is a purely inseparable extension of the latter. Moreover, when V is non-singular and $\Gamma(\varphi(P))_p = 0$, it can be shown that $K' = k(\varphi(P))$.

Using these, the concepts of subvarieties, regular subvarieties, p-regular subvarieties, fields of definitions of these subvarieties and dimensions can be defined as usual. The same is true with the concept of product. Then a point on the product is p-regular if and only if each factor is p-regular. Let $\mathcal{V} \times \mathcal{W}$ be a product of two Q-varieties and $\mathcal{Z}$ a p-regular subvariety of $\mathcal{V} \times \mathcal{W}$ with the projection $\mathcal{Z}'$ on $\mathcal{V}$. The index $[\mathcal{Z} : \mathcal{Z}']$ can be defined in the usual manner. When $\mathcal{Z}' = \mathcal{V}$ and $[\mathcal{Z} : \mathcal{V}] = 1$, we can define a rational map of $\mathcal{V}$ into $\mathcal{W}$. We say that this map is defined at a point ξ if there is a p-regular point $\xi \times \eta$ on $\mathcal{V} \times \mathcal{W}$ such that it is a component of $\xi \times \mathcal{V} \cap \mathcal{Z}$. Using these, we can introduce the concepts of a morphism, a birational correspondence and an isomorphism.

When $\mathcal{V}$ consists entirely of p-regular points, we call it a Q-<u>manifold.</u> When the $\mathcal{V}_i$ are Q-manifolds, finite in number, and the f_{ji} isomorphisms of open subsets of the $\mathcal{V}_i$ into the $\mathcal{V}_j$ such that the graphs of the f_{ji} are closed on the $\mathcal{V}_i \times \mathcal{V}_j$ and that $f_{ji} \circ f_{i\ell} = f_{j\ell}$. Then we can glue the $\mathcal{V}_i$ together by means of the f_{ji} and get an <u>abstract</u> Q-<u>manifold.</u> A subvariety of an abstract Q-manifold may not be an abstract Q-manifold. A subvariety of a Q-manifold may not be a Q-variety. Hence, we define a <u>Q-submanifold</u> of an abstract Q-manifold by means of an abstract Q-manifold and of an injection map. It is on this abstract Q-manifold that we have a complete theory of intersection-multiplicities except for the criterion of multiplicity 1, when we allow the multiplicities to be rational numbers.

Thus, we can deal with a Q-variety as if it is an abstract algebraic variety as far as qualitative problems are concerned. In the same way, we can handle an abstract Q-manifold as if it is a non-singular abstract variety whenever quantitative problems are concerned.

Now it would be clear from Theorems 2 and 3 that the space of moduli (resp. local space of moduli at $\underline{V}$) is a union of a finite set of Q-varieties as soon as a universal damily (resp. local universal family) exists. By Theorem 1 such is the case for polarized surfaces. Moreover, the varieties of moduli of curves and polarized Abelian varieties of bounded rank are Q-manifolds, the latter part of which generalizes Satake's result based on the concept of V-manifolds. Thus, our result c ould be regarded as a basic step in further development of the problems of moduli. But still at this basic level, there are some interesting unsettled problems which are implicitly contained in this note.

THE BOUNDARY OF MODULI SCHEMES

by David Mumford

1° Discussion

To begin with, what is a variety of moduli ? Start with the set of all non-singular complete varieties of dimension n and arithmetic genus p . For each isomorphism class of these, take one point : then try to put these points together in a variety. There are some more requirements : a "nearby" pair of varieties V_1, V_2 should correspond to a "nearby" pair of points : e.g.

Let $\mathcal{S}$ = set of isomorphism classes of V's

$U \subset \mathcal{S}$ is "open", if for all families of varieties of the given type, varieties of type U occur over an open set in the parameter space.

Another requirement is that for all families

$$\pi : \mathcal{V} \longrightarrow S$$

suppose you map S to $\mathcal{S}$ by assigning to each $s \in S$ the class of the fibre $\pi^{-1}(s)$: then this map should be algebraic.

The problem, in this raw form, has been modified bit by bit so as to make it more plausible :

(I.) Instead of classifying "bare" varieties V , one seeks to classify pairs $(V, \mathfrak{D})$ where $\mathfrak{D}$ is a numerical equivalence class of very ample divisors on V .

(II) Then break up the set $\mathcal{S}$ via the Hilbert polynomials of the divisors in $\mathcal{D}$: viz. for every P, let $\mathcal{S}^P$ = isom. classes of $(V, \mathcal{D})$ such that for all $D \in \mathcal{D}$

$$P(n) = \chi(\underline{o}_V(nD)).$$

Now we are close to a good problem :

for all $D \in \mathcal{D}$

for all bases of $H^0(V, \underline{o}_V(D))$ you get a canonical immersion

$$V \subset \mathbb{P}_n \qquad (n = \dim H^0(V, \underline{o}_V(D)) + 1)$$

s.t. hyperplane sections are linearly equivalent to D.

i.e. $\mathcal{S}^P \cong \dfrac{\text{certain set of subvarieties } V \text{ of } \mathbb{P}_n}{\text{certain equivalence relation, especially projective equivalence}}$

(III). Why insist that V be non-singular ? The only reason appears to be that over $\mathbb{C}$ families of non-singular varieties are locally differentiably trivial : so one can view them as families of complex structures on a fixed differentiable maniforld, (or, as in the Bers-Ahlfors approach, on a fixed topological manifold). Algebraically, there is no point : let's let V be any complete variety at all, maybe even reducible and assume that $\mathcal{D}$ is a class of <u>Cartier</u> divisors.

To go further, let's stop and ask what problems arise : first we should take a broad look at the topology which we are getting by throwing in all varieties - typically it will be very un-separated ; second we should try to find open subsets $U \subset \mathcal{S}^P$ such that, in their induced topology, they are separated, and "compact" if possible.

[This means that if U could be given the structure of a moduli variety, it would turn out complete ; and it also means, directly, that if $(V, \mathfrak{D}) \in U$, and we specialize the groundfield, then we can find a specialization $(\overline{V}, \overline{\mathfrak{D}})$ of $(V, \mathfrak{D})$ also in U.]

Thirdly, we will finally have to find out if U can be made into a variety.

(IV.) We understand the last problem better when we realize that, e.g. via chow coordinates, almost all of U is bound to come out as a variety. We saw that $\mathcal{S}^P$ was a quotient of a piece $\mathcal{H}$ of the chow variety by an algebraic equivalence relation. Such quotients always exist birationally, i.e. for a small enough Zariski-open subsets $U^* \subset \mathcal{H}$, [U^*/modulo equivalence relation] will be a good variety. So the 3^{rd} problem is like the first two :

The only problem is to pick the "boundary" components shrewdly, i.e. to decide which non-generic varieties to allow .

there again, it would prejudice the issue to think that we should necessarily use all and/or only non-singular varieties. And the choice should be made by a) checking the topology and b) checking its "algebraizability" .

(V.) A final step in setting up the problem reasonably is to realize that all the same questions occur equally well for a much more general class of problems : viz. that of forming quotients of varieties by algebraic equivalence relations. Only by realizing this can we hope to find simple enough examples to study first so as to get the right feeling. Especially, the hard equivalence relations are tne non-compact one's ; and in the case of moduli, this occurs principally in forming :

$$\mathcal{H} / \{ \text{Projective equivalence of } V\text{'s in } \mathbb{P}_n \}$$

i.e. in forming an orbit space by PGL (n) .

2^o Present State of the Theory

very good (i) analogous problem in classifying vector bundles on a fixed curve

pretty good (ii) moduli of curves (canonically polarized)

half good (iii) moduli of polarized abelian varieties

no good (iv) moduli of surfaces of general type

3° An Example

Rather than analyze an actual moduli problem, I want to take one of the simplest non-trivial orbit space problems, in which all the features of the conjectured results occur !

$G = PGL(1)$ acting on $\mathbb{P}_n$; where $\mathbb{P}_n = n^{th}$ symmetric product of $\mathbb{P}_1$, i.e. $PGL(1)$ acting on theset of 0-cycles of degree n.

(= theory of binary quantics) .

a) jump phenomenon

look at $\mathbb{P}_2/PGL(1)$. There are 2 orbits : $\{P+Q \mid P \neq Q\}$ and $\{2P\}$. Therefore, get 2pts. x, y where x is open but not closed, y is closed but not open :

$$\bullet \longrightarrow \bullet$$

This occurs in all moduli problems, and one always must exclude some points to avoid this.

In $\mathbb{P}_n$, exclude the 0-cycles

$$kP + (n-k)\,Q$$

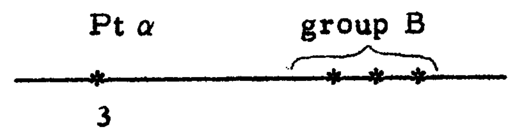
whose isotropy group is infinite.

b) further non-separation

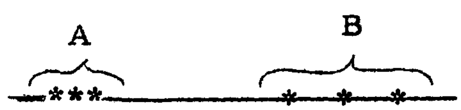
take $n = 6$

generic cycle.

Let all points in group A come together ; you get in the limit :

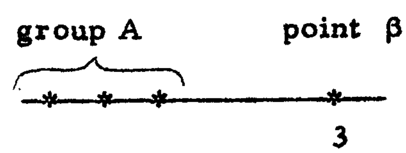
(*) 

But suppose, as group A collapses to α , you apply a one-parameter subgroup $G_m \subset PGL(1)$, moving points away from α to β . Then the following are **projectively equivalent**:



and


the latter approaches :

(**) 

But the 0-cycles (*) and (**) are probably not projectively equivalent.

c) <u>the unitary retraction</u> : to avoid these bad things, define

$$\mathcal{K} \subset \mathbb{P}_n$$

$\mathcal{K}$ = Set of 0-cycles $\sum_{i=1}^{n} P_i$, such that, putting the P_i on the Gauss sphere, and embedding the Gauss sphere in $\mathbb{R}^3$ as $x^2 + y^2 + z^2 = 1$, then the <u>vector</u> sum of the P_i in $\mathbb{R}^3$ is $(0, 0, 0)$.

One checks, if $x, y \in \mathcal{K}$, then x, y are equivalent under $PGL(1)$ if and only if they are equivalent under the maximal compact subgroup

$$K = SO(3; \mathbb{R}) \subset PGL(1, \mathbb{C}) = G .$$

But $\mathcal{K}$ is compact, therefore $\mathcal{K}/K$ is compact and separated. And

$$\mathcal{K} \cdot PGL(1) = \left\{ \mathfrak{A} \;\middle|\; \begin{array}{l} \text{no point } Q \text{ occurs in } \quad \text{with} \\ \text{multiplicity } > n/2 \text{; and if } Q \text{ occurs} \\ \text{with multiplicity } n/2 \text{, then} \\ \mathfrak{A} = \frac{n}{2}(Q+Q') \end{array} \right\} .$$

d) <u>stability restriction</u> : $\mathcal{K} \cdot PGL(1)$ contains a Zariski-open set

$$U_{\text{stable}} = \left\{ \mathfrak{A} \;\middle|\; \begin{array}{l} \text{no point } Q \text{ occurs in } \mathfrak{A} \text{ with} \\ \text{multiplicity } \geqq n/2 \end{array} \right\}$$

So U_{stable}/G has separated topology, and is compact if n is odd. It is also a variety by virtue of a general theorem of mine.

e) <u>semi-stability</u> : when n is even, things are less clean. $\mathcal{K}$ showed that there was a natural compactification of U_{stable}/G by adding a <u>single</u> point representing the cycles $n/2(Q+Q')$. In fact, there is a complete <u>variety</u> $\overline{V}_n$, with point ∞ and diagram of algebraic maps:

$$\begin{array}{ccccc} U_{\text{semi-stable}} & \longrightarrow & & & \overline{V}_n \\ \bigcup & & & & \bigcup \\ U_{\text{stable}} & \longrightarrow & U_{\text{stable}}/G & = & \overline{V}_n - (\infty) \end{array}$$

where

$$U_{\text{semi-stable}} = \left\{ \mathfrak{A} \,\middle|\, \begin{array}{l} \text{no point } Q \text{ occurs in } \mathfrak{A} \text{ with} \\ \text{multiplicity } > n/2 \end{array} \right\} .$$

D. N. Clar

Invariants of a group in an affine ring

by

Masayoshi NAGATA

1. When a group G acts on a ring R inducing a group of automorphisms, then we can speak of G-invariants in R. Let us denote the set of G-invariants in R by $I_G(R)$. Our particular interest lies in the case where R is a finitely generated commutative ring over a field K and the action of G on R is such that 1) the automorphisms are K-isomorphisms and 2) $\Sigma_{g \in G} f^g K$ is a finite K-module for every $f \in R$. In this case, let $f'_1, \ldots, f'_{n'}$ be a set of generators of R over K and choose a linearly independent base $f_1, \ldots, f_n$ of $\Sigma_i (\Sigma_{g \in G} (f'_i)^g K)$. Then $R = K[f_1, \ldots, f_n]$ and the action of F on R is characterized by the representation of G defined by the module $\Sigma_{i,g} f_i^g K$. Thus, in order to observe $I_G(R)$, we may assume that

(1) G is a matric group contained in $GL(n, K)$, and

(2) $R = K[f_1, \ldots, f_n]$ and, for every $g \in G$, the automorphism of R defined by g is induced by the linear transformation

$$\begin{pmatrix} f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_n \end{pmatrix} \longrightarrow g \begin{pmatrix} f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_n \end{pmatrix}.$$

Under the circumstance, the following results are known :

LEMMA 1.1. $I_G(R)$ is finitely generated if every rational representation of G is completely reducible or if G is a finite group, hence if G has a normal subgroup N of finite index such that every rational representation of N is completely reducible.

In the general case, there are some examples of a pair of G and R such that $I_G(R)$ is not finitely generated.

LEMMA 1.2. If $\bar{G}$ is the smallest algebraic set in $GL(n, K)$ among those containing G, then $\bar{G}$ is a group which acts on R naturally and $I_G(R) = I_{\bar{G}}(R)$.

LEMMA 1.3. If K' is a ring containing K, then, under a natural extension of the action of G on $R \otimes_K K'$ such that every element of K' is G-invariant, we have $I_G(R \otimes_K K') = I(R) \otimes_K K'$.

By virtue of Lemmas 1.2, 1.3 above, we see that, in asking finite generation of $I_G(R)$, fundamental is the case where G is an algebraic group with universal domain K. But, such an assumption does not bring us any simplicity in our treatment. Therefore we shall not assume that G is an algebraic group, but assume the assumptions (1) and (2) above.

Furthermore, rational representations of G which we meet in our treatment are rather special, and therefore it is good enough to understand by a rational representation of G a representation obtained in the following manner :

Let R^* be the polynomial ring over K in indeterminates $X_1, \ldots, X_n$. Then G acts on R^* as defined by

$$\begin{pmatrix} X_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ X_n \end{pmatrix} \longrightarrow g \begin{pmatrix} X_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ X_n \end{pmatrix} \qquad \text{for each } g \in G .$$

Let M and N be G-stable finite K-modules contained in R^* such that $N \subseteq M$. M/N defines a rational representation of G. Rational representations we shall meet with in this paper are those of this type.

2. We call G a <u>reductive group</u> if every rational representation of G is completely reducible. It is known that

LEMMA 2.1. If G is an algebraic group, then (i) in the characteristic zero case, the reductivity is equivalent to the condition that the radical is a torus and (ii) in the case of characteristic $p \neq 0$, the reductivity is equivalent to the condition that the connected component G_0 of the identity of G is a torus and furthermore the index $(G : G_0)$ is prime to p.

Thus the class of reductive groups is not very small in the characteristic zero case, but is very small in the positive characteristic case. Thus, in view of the known counter-example to the 14-th problem of Hilbert, the following consequence of Lemma 1.1 is rather satisfactory in the characteristic zero case and is very unsatisfactory in the positive characteristic case :

LEMMA 2.2. In the characteristic zero case, $I_G(R)$ is finitely generated if the radical of the smallest algebraic group $\overline{G}$ in $GL(n, K)$ among those containing G is a torus : in the positive characteristic case, $I_G(R)$ is finitely generated if the connected component of the identity of $\overline{G}$ is a torus.

3. Let us denote by P_m from now on the polynomial ring over K in n indeterminates $X_1, \ldots, X_m$.

Let ρ be a rational representation of G. If $\rho(G) \subseteq GL(m, K)$, then we define an action of G on P_m by

$$\begin{pmatrix} X_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ X_m \end{pmatrix} \to \rho(g) \begin{pmatrix} X_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ X_m \end{pmatrix} \quad \text{for every } g \in G .$$

We call G a <u>semi-reductive group</u> if the following is true : If ρ is a rational representation of G which defines an action on P_m (m being such that $\rho(G) \subseteq GL(m, K)$) such that (i) $\Sigma_{i \geq 2} X_i K$ is G-stable and (ii) X_1 modulo $\Sigma_{i \geq 2} X_i K$ is G-invariant, then there is a polynomial $F \in P_m$ which is G-invariant, monic in X_1 and of positive degree in X_1.

Since the action of G preserves the degree of every homogeneous form, the condition on F above may be replaced by the condition to be a G-invariant homogeneous form of positive degree which is monic in X_1.

For algebraic linear groups, it was conjectured by D. Mumford that if the radical is a torus then the group is semi-reductive. As will be shown below, this conjecture is equivalent of the following, which we like to call Mumford Conjecture :

Mumford Conjecture. If G is a connected semi-simple algebraic linear group, then G is semi-reductive.

To the writer's knowledge, Mumford Conjecture has been solved only in a very special case where characteristic is 2 and $G = SL(2, K)$; it was done by Mr. Tadao Oda.

The purpose of the present note is to show

MAIN THEOREM. $I_G(R)$ is finitely generated if G is semi-reductive.

Let us indicate here how to prove the equivalence of Mumford conjecture with the case of an algebraic group whose radical is a torus. The key lemma is :

LEMMA 3.1. Let N be a normal subgroup of G. If both N and G/N are semi-reductive, then G is also semi-reductive.

<u>Proof:</u> Let ρ be a rational representation of G as stated in the definition of semi-reductivity. Then the restriction ρ' of ρ on N is of the same type, whence there is a homogeneous form $F \in P_m$ of positive degree such that F is monic in X_1 and N-invariant under the action of N defined by ρ'. Consider the G-module $M = \Sigma_{g \in G} F^g K$. The action of G on M is really an action of G/N. Let M^* be $M \cap \Sigma_{i \geq 2} X_i P_m$, and let $F_1, \ldots, F_s$ be a base of M^*. Then, since $M = FK + M^*$, since any power of X_1 is G-invariant modulo $\Sigma_{i \geq 2} X_i P_m$, the semi-reductivity of G/N implies the existence of a homogeneous form F^* in $F, F_1, \ldots, F_s$ of positive degree such that (i) it is monic in F and (ii) it is G-invariant. F^* is a homogeneous form of positive degree in $X_1, \ldots, X_m$. Since $F_i \in \Sigma_{j \geq 2} X_j P_m$ and since F is monic in X_1, we see that F^* is monic in X_1. Thus G is semi-reductive.

Now the equivalence said above is proved easily by the fact that finite groups and tori are all semi-reductive.

4. Before proving our main theorem, we like to give a remark on our formulation of Mumford Conjecture. Mumford's formulation was stated in projective space. Namely, if ρ is a rational representation of G and if $\rho(G) \subseteq GL(m, K)$, then an action of G on P_m is defined, which defines an action of G on the projective space S^{m-1} of dimension $m-1$. The condition proposed by Mumford is that if a point $P \in S^{m-1}$ is G-invariant, then there is a G-stable hypersurface in S^{m-1} which does not go through P.

If this condition is stated in P_m, then, choosing coordinates of P to be $(1, 0, \ldots, 0)$, it can be stated as follows :

If $\Sigma_{i\geq 2} X_i K$ is G-stable (hence, X_1 modulo $\Sigma_{i\geq 2} X_i K$ is G-semi-invariant), then there is a G-semi-invariant homogeneous form F which is monic in X_1 and of positive degree.

PROPOSITION 4.1. If the above condition is satisfied by G, then G is semi-reductive.

Proof: Let ρ be as in the definition of semi-reductivity. Then there is a homogeneous form F as in the above condition. Since X_1 is invariant modulo $\Sigma_{i\geq 2} X_i K$ under the action of G, any power of

X_1 is G-invariant modulo the ideal generated by $\Sigma_{i \geq 2} X_i K$. Therefore that F is G-semi-invariant implies that F is G-invariant.

The converse of Proposition 4.1 is also true, and was proved by Mr. M. Miyanishi. The proof will be given at the end of this article as an appendix.

5. A reductive group is obviously a semi-reductive group, hence our main theorem includes the corresponding result for reductive groups. As for the proof, that special case is much simpler than the semi-reductive case. In order to compare these cases, let us begin with glance at the reductive case.

The following two are key lemmas to prove our main theorem for reductive groups :

LEMMA 5.1. A. Let ϕ be a G-homomorphism from R onto a ring R'. If G is reductive, then $I_G(R') = \phi(I_G(R))$.

LEMMA 5.2. A. If G is reductive, then for any $h_1, \ldots, h_s$ in $I_G(R)$, we have $(\Sigma_i h_i R) \cap I_G(R) = \Sigma_i h_i (I_G(R))$.

Namely, the first lemma enables us to assume that $f_1, \ldots, f_n$ are algebraically independent. Then the second lemma shows that $I_G(R)$ is a graded Noetherian ring, and we see easily that $I_G(R)$ is finitely generated, by virtue of a well known lemma which will be recalled later.

For semi-reductive groups, we have the following adaptions of the above lemmas :

LEMMA 5.1. B. With the same notations as above, if G is semi-reductive, then, for every element x of $I_G(R')$, there is a power x^t of x such that $x^t \in \phi(I_G(R))$. Consequently, $I_G(R')$ is integral over $\phi(I_G(R))$ in this case.

LEMMA 5.2. B. Assume that G is semi-reductive. Then for any $h_1, \ldots, h_s \in I_G(R)$, every element of $(\Sigma_i h_i R) \cap I_G(R)$ is nilpotent modulo $\Sigma_i h_i(I_G(R))$.

Proof of Lemma 5.1.B : Let y be an element of R such that $\phi(y) = x$. Set $M = \Sigma_{g\in G} y^g K$, $\mathfrak{a} = \phi^{-1}(0)$, $N = M \cap \mathfrak{a}$. If $x = 0$, then the assertion is obvious, and we assume that $x \neq 0$. Since x is G-invariant, we have $y^g - y \in N$ for every $g \in G$. Therefore, letting $y_1, \ldots, y_m$ be a linearly independent base of N, we see that, by virtue of the semi-reductivity of G, there is a G-invariant element F of $K\{y, y_1, \ldots, y_m\}$ which is monic and of positive degree, say t, in y, and homogeneous in $y, y_1, \ldots, y_m$. Then $\phi(F) = x^t \in \phi(I_G(R))$. This completes the proof of Lemma 5.1.B .

Proof of Lemma 5.2.B. We shall make use of induction argument on s without fixing R. Let ϕ be the natural homomorphism from R onto R/h_1R. Let x be an arbitrary element of $(\Sigma_i h_iR) \cap I_G(R)$. Then $\phi(x)$ is in $\Sigma_{i\geq 2}\phi(h_i)\phi(R) \cap \phi(I_G(R))$, whence by induction on s, we see that there is a natural number t such that $\phi(x^t)$ is in $\Sigma_{i\geq 2}\phi(h_i)I_G(\phi(R))$. This means that $x^t = \Sigma_i h_iF_i$ with $F_1 \in R$ and $F_2, \ldots, F_s \in \phi^{-1}(I_G(\phi(R))$. By Lemma 5.1.B, there is a natural number u such that $\phi(F_s u) \in \phi(I_G(R))$. Then, considering x^{tu} instead of x^t, we may assume that $F_s \in I_G(R)$ (if $s > 1$). Then $X^t - h_sF_s \in (\Sigma_{i\leq s-1}h_iR) \cap I_G(R)$, and $x^t - h_sF_s$ is nilpotent modulo $\Sigma_{i\leq s-1}h_i(I_G(R))$, which implies the assertion. Therefore we have only to prove the case where $s = 1$. In this case, $x = h_1x'$ with $x' \in R$ and x' is G-invariant modulo $0 : h_1R$. Let σ be the natural homomorphism $R \longrightarrow R/(0 : h_1R)$. Then $\sigma(x') \in I_G(\sigma(R))$, whence there is a natural number t such that $\sigma(x'^t) \in \sigma(I_G(R))$. Let $z \in I_G(R)$ be such that $\sigma(z) = \sigma(x'^t)$. Then $x^t = h_1{}^t x'^t = h_1{}^t z \in h_1(I_G(R))$. This completes the proof of Lemma 5.2.B.

We recall here the lemma on graded Noetherian ring refered above :

LEMMA 5.3. Assume that a ring A is such that (i) it is the direct sum of submodules $A_0, A_1, \ldots, A_n, \ldots$ and (ii) $A_iA_j \subseteq A_{i+j}$ for every possible pair (i,j). If the ideal $\Sigma_{i \geq 1} A_i$ has a finite basis, then A is finitely generated over A_0.

6. Let ϕ be the homomorphism from P_n onto R such that $\phi(X_i) = f_i$ for every i and let $\mathfrak{k}$ be the kernel of ϕ. We shall prove here the main theorem in the case where $\mathfrak{k}$ is a homogeneous ideal. Since P_n is Noetherian, we can use induction argument on the largeness of $\mathfrak{k}$. Thus we assume that if $\mathfrak{k}'$ is a G-stable homogeneous ideal of P_n and contains $\mathfrak{k}$ properly, then $I_G(P_n/\mathfrak{k}')$ is finitely generated.

LEMMA 6.1. Under the circumstance, if $\mathfrak{h}$ is a graded ideal $\neq 0$ of R, then $I_G(R)/(\mathfrak{h} \cap I_G(R))$ is finitely generated.

Proof: By assumption, $I_G(R/\mathfrak{h})$ is integral over $I_G(R)/\mathfrak{h} \cap I_G(R))$. These two facts show the result.

Therefore, by virtue of Lemma 5.3, if there is such an ideal $\mathfrak{h}$ (not containing 1) as above so that $\mathfrak{h} \cap I_G(R)$ has a finite basis, then we see the finite generation of $I_G(R)$.

As a particular case, we have the case of an integral domain. Namely if h is a homogeneous element of $I_G(R)$ and if R is an integral domain, then $hR \cap I_G(R) = h(I_G(R))$. The same reasoning is applied if there is a homogeneous element h of positive degree which is not a zero divisor.

Next we consider the case where R is not an integral domain. Let $h \neq 0$ be a homogeneous element of $I_G(R)$ of positive degree. Set $\mathfrak{a} = 0 : hR$. If $\mathfrak{a} = 0$, then we finished already, and we assume that $\mathfrak{a} \neq 0$. Then, by Lemma 6.1, both $I_G(R)/(hR \cap I_G(R))$ and $I_G(R)/(\mathfrak{a} \cap I_G(R))$ are finitely generated. Therefore there is a finitely generated subring A of $I_G(R)$ such that $I_G(R)/(hR \cap I_G(R)) = A/(hR \cap A)$ and such that $I_G(R)/(\mathfrak{a} \cap I_G(R)) = A/(\mathfrak{a} \cap A)$. Since $I_G(R/\mathfrak{a})$ is a finite module over $A/(\mathfrak{a} \cap A)$, there are elements $c_1, \ldots, c_t$ of R such that $I_G(R/\mathfrak{a})$ is generated by these c_i modulo $\mathfrak{a}$ as an $A/(\mathfrak{a} \cap A)$-module. We like to show that $I_G(R)$ is then generated by $c_i h$ over A. Since c_i modulo $\mathfrak{a}$ are G-invariant, we see that $c_i h$ are G-invariant. Conversely, let x be any element of $I_G(R)$. Then there is an element a of A such that $x - a \in hR$. Let r be such that $x - a = hr$ $(r \in R)$. Since hr is G-invariant, we see that r modulo $\mathfrak{a}$ is G-invariant, whence there is an element b of ΣAc_i such that $r - b \in \mathfrak{a}$. Then $hr = hb \in A[hc_1, \ldots, hc_t]$ this completes the proof, provided that the kernel $\mathfrak{k}$ of ϕ is homogeneous.

7. Now we consider the general case. We adapt the notation is § 6 without assuming that $\mathfrak{k}$ is homogeneous. The induction argument is also adapted, considering all G-stable ideals of P_n. Then we need a different proof only in the case where $I_G(R)$ is an integral domain (for, otherwise, take an element h of $I_G(R)$ which is a zero-divisor in

$I_G(R)$, and adapt the proof just above) . In this case, $I_G(R)$ is integral over $I_G(P_n)/((k) \cap I_G(P_n))$. Since the result in § 6 includes the case where $k = 0$, we see that $I_G(P_n)$ is finitely generated, hence the integral dependence implies that $I_G(R)$ is finitely generated. Thus the proof of the main theorem is completed.

APPENDIX

by Masayoshi Miyanishi

We shall prove here the converse of Proposition 4.1 above. Assume that a rational representation ρ of G is of the form

$$\begin{pmatrix} t & \sigma \\ 0 & \rho' \end{pmatrix}$$

where t is of degree 1. Let m be the degree of ρ. Then we consider a representation $\tau = tE$, E being the unit matrix of degree m. Then $\tau(g)$ is in the center of $GL(m, K)$ for every $g \in G$, and therefore $\rho\tau^{-1}$ gives a rational representation of G (not in the restricted sense above, but in the usual sense). By the semi-reductivity of G, there is a homogeneous form F in P_m of positive degree such that it is monic in x_1 and G-invariant under the action of G defined by $\rho\tau^{-1}$. Then F is semi-invariant under the action of G defined by ρ. This proves the converse of Proposition 4.1.

TRANSFORMATION SPACES, QUOTIENT SPACES, AND SOME CLASSIFICATION PROBLEMS.

Maxwell Rosenlicht

For simplicity let us restrict our attention to varieties in the classical sense. If V is a variety and $R \subset V \times V$ is an equivalence relation among the points of V, by a quotient variety is meant a pair $(V/R, p)$, where V/R is a variety and $p: V \longrightarrow V/R$ is a surjective morphism such that two points of V have the same image under p if and only if they are R-equivalent and such that, for any $v \in V$, if f is a rational function on V that is defined at v and is R-invariant (i.e., constant on R-equivalence classes) then f is the composition of a rational function on V/R that is defined at px and the map p [1, exposé 8]. If V/R exists, it clearly satisfies a universal mapping property for R-invariant morphisms of V and, in particular, is essentially unique. However V/R need not exist: one necessary condition for the existence of V/R is that R be a closed subset of $V \times V$.

In what follows, we consider only the case where V is a transformation space for an algebraic group G and

$$R = \{(v, gv) \mid v \in V, g \in G\}$$

is the equivalence relation whose equivalence classes are the G-orbits on V; in this case it is customary to write V/G instead of V/R

(if this exists). If V/G exists, the map $p : V \longrightarrow V/G$ is automatically separable, for the function field on V/G is the subfield of the function field on V consisting of all elements left fixed by a group of automorphisms. In general, the graph of the operation of G on V is a closed subset of $G \times V \times V$ so that R, the projection of this graph on $V \times V$, is always constructible. The isotropy groups (stability groups) of the points of V can be obtained by intersections on $G \times V \times V$, hence have the obvious semicontinuity property that the dimension of the isotropy subgroup of $v \in V$ is constant for v on a certain G-invariant open subset of V, and greater than this constant on the complementary closed subset. Any given point of V has an orbit and an isotropy group the sum of whose dimensions is dim G, so that all orbits on a certain G-invariant dense open subset of V have the same dimension, and all other orbits have strictly smaller dimension. If it should happen that all orbits have the same dimension, then the fact that the closure of an orbit is also G-invariant would imply that all orbits are closed. However all orbits may be closed without equidimensionality holding; e.g., if G is unipotent and V affine, orbits need not have the same dimension but they are always closed [3]. If R is closed then the equation

$$v \times Gv = R \cap (v \times V)$$

implies that all orbits on a dense open G-invariant subset of V have constant dimension, with other orbits having larger dimension; thus if R is closed, in particular if V/G exists, all orbits are closed and have equal dimension.

If a quotient $p : V \longrightarrow V/G$ exists, a number of other pleasant consequences follow without any further assumption [3]. In this case the map p is open, so that V/G has the expected quotient topology. If $V' \subset V$ is open and G-invariant then the subset V'/G of V/G is a quotient variety of V'. If W is any variety and G operates on $V \times W$ by the rule $g(v,w) = (gv,w)$, then $(V \times W)/G$ exists and equals $(V/G) \times W$. There is not much of a theory on fields of definition, for if G and V are defined over the field k and if V/G is quasi-projective (a condition that can be relaxed somewhat), then V/G and p may both be chosen so as to be defined over k.

The existence of a quotient V/G turns out to be largely a local problem, for if V is covered by G-invariant open subsets $\{V_i\}$ such that each V_i/G exists, then V/G exists if and only if R is closed. But the closure of R does not insure the existence of V/G, as an example of Nagata shows [2]. Good local criteria for the existence of quotients are much to be desired. The most general result in this direction is due to Seshadri [8]. The most important case of Seshadri's result is when V is a principal transformation variety for G, i.e., when R is closed, all isotropy groups are points, and the map $R \longrightarrow G$ given by $(v, gv) \rightsquigarrow g$ is a morphism, and it says that if V is normal then each of its points has a G-invariant open neighborhood which has a finite galois covering which is also a principal space for G and in addition admits a quotient by G (so that the existence of V/G depends locally on the existence of quotients for finite groups operating on other varieties). Seshadri has also shown [9] that if V is a normal principal space for an abelian variety G then V/G always exists.

As might be expected, the simplest general result on the existence of quotient varieties is also one of the most useful. It is to the effect that for any transformation space V for the algebraic group G there exists a dense G-invariant open subset V' of V such that V'/G exists [6]. The proof consists in first constructing V/G and p birationally, by means of the G-invariant rational functions on V, and then cutting off closed subsets that cause trouble. In case R is closed, it is immediate that there exists a unique maximal G-invariant open subset V' of V such that V'/G exists. If there exist sufficiently many G-automorphisms of V then V/G will exist, a result which produces a very easy proof of the existence of coset spaces for subgroups of groups, together with all the desired structure and rationality properties of these quotients [4].

There are a number of important results stating that if V is affine and certain other conditions hold then V/G exists and is also affine. In such cases the coordinate ring on V/G must consist of all G-invariant functions in the coordinate ring of V, which gives the starting point of all the proofs, and practically the whole proof in the case where G is finite [7, pp. 57 - 59]. (If G is finite there is an immediate generalization giving the existence of V/G where V is not affine, but each orbit on it is contained in an affine open subset [7] ; an example of Nagata for $G = Z/2Z$ shows that this result may fail without the last condition.) The result holds whenever G is a torus and orbits are equidimensional [3], and also if G is reductive and all orbits are closed, at least in the case of characteristic zero (Borel, Iwahori, Mumford, Nagata).

There are interesting problems connected with the classification of transformation spaces for algebraic groups, even in the special case where the transformation space is homogeneous or prehomogeneous (i.e., has a dense homogeneous subset) and the group is connected and solvable. If V is homogeneous and G is commutative then, fixing a point of V, V is simply an algebraic group that is a homomorphic image of G, while if G is connected, solvable and linear, then V is isomorphic (as an algebraic set) to a product of affine lines and affine lines with single points deleted [5]. In the last case, if G and V are defined over a field k such that G is k-solvable (meaning, roughly, that G has a composition series over k with all quotient groups isomorphic to the additive or multiplicative group in one variable), then this product decomposition of V can be done rationally over k. In the special case where $\dim G = 1$ the result, even without the rationality part, leads to an easy proof that for any quotient variety $V \longrightarrow V/G$, where G is connected, solvable, and linear, there exists a rational cross-section

$V/G \longrightarrow V$.

The problem of classifying all complete prehomogeneous spaces for connected unipotent groups derives its main interest from the fact that if B is a Borel subgroup of a connected linear algebraic group G then G/B is prehomogeneous for B_u (and furthermore there are only a finite number of orbits, each isomorphic to an affine space). In the same way the operation of a maximal torus T of G on G/B leads one to consider in full generality projective varieties V that are transformation spaces for a torus T, theorems which enable one to read off a good deal of the classification theory of linear algebraic groups [1, exposé 10 ff.]. For example, one can prove easily that the fixed points for T on V are at least $\dim V + 1$ in number and all of V is left fixed by a subtorus of T of codimension $\leq \dim V$, which two facts together almost imply that a semisimple linear algebraic group is generated by its 3-dimensional simple subgroups.

REFERENCES

[1] C. Chevalley, Classification des groupes de Lie algébriques, Séminaire E.N.S., Paris , 1958.

[2] M. Nagata, Note on orbit spaces, Osaka Math. J., vol. 14 (1962).

[3] M. Rosenlicht, On quotient varieties and the affine embedding of certain homogeneous spaces, Trans. Amer. Math. Soc., vol. 101 (1961).

[4] __________, The definition of field of definition, Bol. Soc. Mat. Mex. (19

[5] __________, Questions of rationality for solvable algebraic groups over nonperfect fields, Annali di Mat., vol. 61 (1963).

[6] __________, A remark on quotient spaces, to appear in Anais da Academia Brasileira de Ciencias.

[7] J.-P. Serre, Groupes algébriques et corps de classes, Paris, 1959.

[8] C. S. Seshadri, Some results on the quotient space by an algebraic group of automorphisms, Math. Ann., vol. 149 (1963) .

[9] __________, Quotient space by an abelian variety, Math. Ann., vol. 159 (1963).

ON THE THEORY OF COMPACTIFICATIONS

Jun-Ichi Igusa

This is the first part of our lecture, "On the Siegel modular variety", and it contains an outline of a proof of the fact that compactification of Satake's type [1] have, under certain general conditions, no finite non-singular coverings locally at the boundary points. This fact was observed in the case of the compactifications of the Siegel upper-half plane of genus two [5, cf. 7]. However, the proof we had in that case was too special. Following a suggestion given to us by Zariski, with the use of our results on "theta-constants" we then examined the compactification of the Siegel upper-half plane of arbitrary genus and found the under-lying mechanism, which we find convenient to explain using the theory of "Siegel domains of the third kind" developed by Pyatetski-Shapiro [10]. We shall, therefore, start summarizing Pyatetski-Shapiro's results (making a minor correction) to increase the readability.

1. Let T be a bounded domain, i.e., a non-empty bounded connected open subset of a complex vector space, or at least (complex) analytically isomorphic to a bounded domain, and let U, Z be complex

---

1. This means the compactifications of quotient varieties of bounded symmetric domains (by certain properly discontinuous groups of analytic automorphisms) which are obtained by "adding" quotient varieties of some boundary components (using Cartan's theorem on the prolongation of normal analytic spaces [2]). A most general theory of compactifications (of Satake's type) has recently been obtained by Baily and Borel.

vector spaces all three of finite dimensions. Let R be a "real subspace" of Z, i.e., a subspace of Z when Z is considered as a vector space over $\mathbb{R}$, such that Z splits into a direct sum of R and iR : $Z = R + iR$, $R \cap iR = 0$. If z is a vector in Z, it can be written uniquely in the form $\mathrm{Re}(z) + i\mathrm{Im}(z)$ with $\mathrm{Re}(z), \mathrm{Im}(z)$ in R. We shall assume that a non-empty open convex cone C which contains no entire straight line is given in R. This means that, with respect to a suitable affine coordinate system in R, C is contained in the first quadrant. We shall assume that, for every point t of T, a "quasi-hermitian form" $L_t : U \times U \longrightarrow Z$ is given. This means that $L_t(u, v)$ is $\mathbb{C}$-linear in u, $\mathbb{R}$-linear in v and

$$[u, v] = (1/2i)(L_t(u, v) - L_t(v, u))$$

is "real", i.e., R-valued. We then consider the set S of points in the product $Z \times U \times T$ with coordinates (z, u, t) satisfying

$$\mathrm{Im}(z) - \mathrm{Re}(L_t(u, u)) \in C .$$

We shall impose further conditions. We require first that the mapping $U \times T \longrightarrow R$ given by $(u, t) \longrightarrow \mathrm{Re}(L_t(u, u))$ is continuous. This implies that S is an open subset of $Z \times U \times T$. We then require that S is analytically isomorphic to a bounded domain. The third condition is more involved. We consider the set $\mathcal{U}$ of analytic mappings $b : T \longrightarrow U$ such that the mapping $T \longrightarrow Z$ defined by $t \longrightarrow L_t(u, b(t))$ is also analytic for every u in U. This implies that the mapping $T \times T \longrightarrow Z$ defined by $(t, t') \longrightarrow L_t(b(t'), b(t))$ is analytic. At any rate, it is clear that $\mathcal{U}$ forms a vector space over $\mathbb{R}$. We require that $\mathcal{U}$ and U have the same dimension over $\mathbb{R}$. As it was shown by Pyatetski-Shapiro, this means that, if t_0 is an arbitrary point of T, the mapping $\mathcal{U} \longrightarrow U$ defined by $b \longrightarrow b(t_0)$ is an isomorphism over $\mathbb{R}$. If these conditions are satisfied, we say that S is a <u>Siegel domain</u> (of the third kind) over T.

Suppose that S is a Siegel domain over T. Then, for (b,a) in $\mathcal{U} \times R$, the mapping $(b,a) : S \longrightarrow S$ defined by

$$(z,u,t) \longrightarrow (z + a + iL_t(2u + b(t), b(t)), \; u + b(t), \; t)$$

is an analytic automorphism of S. These automorphisms of S form a subgroup G_3 of the group G_0 of all analytic automorphisms of S. The law of composition in G_3 is given by

$$(b,a)(b',a') = (b + b', \; a + a' + 2[b,b']) .$$

We note, here, that the mapping $[b,b'] : T \longrightarrow Z$ can be identified with an element of R, because it is analytic and R-valued, hence constant. We also make the following observation. Consider the fiber over t, say S_t, of the fibering $S \longrightarrow T$ defined by $(z,u,t) \longrightarrow t$. Consider further the fibering $S_t \longrightarrow C$ defined by $(z,u,t) \longrightarrow \mathrm{Im}(z) - \mathrm{Re}(L_t(u,u))$. This fibering has a global cross-section defined by $r \longrightarrow (ir, 0, t)$ and the fiber bundle $S_t \longrightarrow C$ is isomorphic to the product-bundle $G_3 \times C \longrightarrow C$ in an obvious way. Since G_3 operates on each fiber as left translations, it is called the <u>group of translations</u> in S. In the following, we shall assume that the skew-symmetric bilinear form $[b,b']$ is <u>non-degenerate.</u> It is the same thing to assume that the center G_4 of G_3 is the subgroup defined by $b = 0$.

This assumption is always satisfied in the applications. Since G_4 is isomorphi to R as $a \longrightarrow (0, a)$, it will be identified with R. Then we have an isomorphism $G_3/R \simeq \mathcal{U}$ induced from $(b, a) \longrightarrow b$. We recall that, at each point t_0 of T, we have an isomorphism $\mathcal{U} \simeq U$ over $\mathbb{R}$ defined by $b \longrightarrow b(t_0)$. If Ω is a subgroup of G_3, we shall denote its image in U under the composite mapping simply by $\Omega(t_0)$.

We shall also define G_1 and G_2. Consider the group of analytic automorphisms of S of the following form

$$(z, u, t) \longrightarrow (Az + a(u, t), \ B(t)u + b(t), \ g(t)) \ ,$$

in which g represents analytic automorphisms of T. They form a subgroup of G_0, and this is G_1. As for G_2, it is the normal subgroup of G_1, defined by $g = \mathrm{id}$. It is clear that $G_0, G_1, \ldots$ form a decreasing sequence. Using a classical terminology in the theory of Fuchsian groups, G_1 is called the <u>group of parabolic transformations</u> in S. A complete description of G_2 will now be given. In general, if L is an arbitrary quasi-hermitian form, it can be expressed uniquely as a sum of a hermitian form and a symmetric form. For instance, the hermitian part H of L is given by

$$H(u, v) = (1/2i)(L(iu, v) - L(u, iv)) \, .$$

We shall denote the hermitian part of L_t by H_t. This being remarked, if

$$(z, u, t) \longrightarrow (Az + a(u, t) \, , \ B(t)u + b(t) \, , \ t)$$

is an arbitrary element of G_2, it decomposes uniquely into a product $(b, a)\gamma$ of (b, a) and γ with γ given explicitly as

$$(z, u, t) \longrightarrow (Az - iAL_t(u, u) + iL_t(B(t)u, B(t)u), B(u)u, t),$$

in which A, $B(t)$, $b(t)$ have the same meaning as in the original element of G_2. We note that necessary and sufficient conditions for a transformation like that of γ to define an analytic automorphism of S are

(1) A <u>is an element of</u> $GL(Z)$ <u>satisfying</u> $AC = C$,

(2) $B : T \longrightarrow GL(U)$ <u>is analytic</u>,

(3) $AH_t(u, u) = H_t(B(t)u, B(t)u)$ <u>for all</u> (u, t) in $U \times T$.

Furthermore, elements like γ form a subgroup $\{\gamma\}$ of G_2, and it is isomorph to the group of pairs (A, B) satisfying the above three conditions. In Pyatetski-Shapiro, the exact form of γ and the crucial condition (3) are stated incorrectly. At any rate, G_3 is the normal subgroup of G_2 defined by $A = id.$, $B = id.$, and we have a semidirect product decomposition $G_2 = G_3 \cdot \{\gamma\}$. Moreover, the law of composition in G_2 is described as

$$((b, a)\gamma)(b', a')((b, a)\gamma)^{-1} = (Bb', Aa' + 4[b, Bb']).$$

2. Using the same notations as in the previous section, we shall introduce a Hausdorff topology in the union $\bar{S} = S \cup T$ so that S becomes an open subset of $\bar{S}$. We have only to assign neighborhoods to each point of T. Let t_0 be a point of T. We take a neighborhood V of t_0 in T and a vector r of R. We then consider the subset $S(V, r)$ of S defined by

$$Im(z) - Re(L_t(u, u)) - r \in C, \quad t \in V$$

and take the union $\bar{S}(V, r) = S(V, r) \cup V$ as a neighborhood of t_0 in $\bar{S}$. It is easy to verify that we have a topology in $\bar{S}$ with the required properties. We observe that G_2 operates on $\bar{S}$ as a group of homeomorphisms. In fact we have

$$(b, a)\gamma . S(V, r) = S(V, Ar) .$$

It is also immediate to introduce the structure of a normal ringed space in $\bar{S}$ which induces on S the given structure of the complex analytic manifold.

Now, every element of G_1 gives rise to an analytic automorphism of T as $t \longrightarrow g(t)$. In this way G_1/G_2 can be identified with a subgroup of the group of analytic automorphisms of T. Let Γ_0 be a subgroup of G_0 which is properly discontinuous on S. We shall assume that T is "Γ_0-rational". If we put $\Gamma_k = \Gamma_0 \cap G_k$ for $k = 1, 2, \ldots,$ this means that the quotient space G_3/Γ_3 is compact and that the quotient group Γ_1/Γ_2 is properly discontinuous on T. Since we do not know whether it is a consequence or not, we shall assume, in addition, that if we take V sufficiently small and r sufficiently "large", elements α of Γ_0 with the property $\alpha \cdot S(V, r) \cap S(V, r) \neq \emptyset$ are all contained in Γ_1. We know that this assumption is always satisfied if S is obtained from a bounded symmetric domain and from its boundary component. This being remarked, we take a point t_0 of T which is <u>not</u> a fixed point of Γ_1/Γ_2, and investigate the compactification of the quotient variety of S by Γ_0, which we shall denote simply by S/Γ_0, around the image point of t_0.

In general, let Ω be a discrete subgroup of G_3 such that the quotient space G_3/Ω is compact. It is the same thing to assume that G_3/Ω has a finite volume. We note that the bi-invariant measure in G_3 is the product measure of the ordinary measures in $\mathcal{U}$ and R. At any rate, if Ω is such a group, then $\Omega \cap R$ is discrete in R and the image $\Omega(t)$ of Ω in U is discrete in U for every t both with compact quotient groups. Therefore, if f is an analytic function in $S(V, r)$ and if it is invariant by $\Omega \cap R$, i.e., by the operations of $\Omega \cap R$, it admits a Fourier expansion

$$f(z, u, t) = \sum_{\rho} \theta_{\rho}(u, t)\, e(\rho(z)),$$

in which $\rho : Z \longrightarrow \mathbb{C}$ is $\mathbb{C}$-linear and takes integer values on $\Omega \cap R$. Actually, the series is absolutely and uniformly convergent in every compact subset of $S(V, r)$, and the coefficients define analytic functions on $U \times V$. Furthermore, in case f is invariant by Ω, each θ_{ρ} satisfies the functional equation

$$\theta_{\rho}(u + b(t), t) = e(-\rho(a + iL_t(2u + b(t), b(t))))\theta_{\rho}(u, t)$$

for all (b, a) in Ω. Therefore, for each t in V, the function $u \longrightarrow \theta_{\rho}(u, t)$ is a <u>theta-function</u> (or a "Jacobi function") on U relative to $\Omega(t)$. In particular $\theta_0(u, t)$ depends only on t. The Fourier expansion of $z \longrightarrow f(z, u, t)$ is called the <u>Fourier-Jacobi series</u> of f by Pyatetski-Shapiro. It is easy to determine the <u>Riemann form</u> of θ_{ρ}, more precisely of $u \longrightarrow \theta_{\rho}(u, t)$, in the sense of Weil [12]. In fact, it is simply the hermitian part of the quasi-hermitian form $2i \cdot (-\rho(iL_t(2u, v)))$. Therefore the Riemann form of θ_{ρ} is $4\rho(H_t(u, v))$, and its imaginary part is $4\rho([u, v])$. We note that $4\rho([u, v])$ is integer valued on $\Omega(t) \times \Omega(t)$. In fact ρ takes integer values on $\Omega \cap R$ and, with $b(t)$, $b'(t)$ in $\Omega(t)$, $4[b, b']$ is in $\Omega \cap R$ because of the last formula in Section 1. On the other hand, since the Riemann form has to be positive semi-definite, the summation in the Fourier-Jacobi series of f is restricted by

$$\rho(H_t(u, u)) \geq 0$$

for all u in U. This in general implies that ρ is non-negative on C. On the other hand, if f is bounded in $S(V, r)$ and if $\rho \neq 0$ appears in the Fourier-Jacobi series of f, then ρ is positive on C. (The converse is also true when V is relatively compact with respect to T.) Therefore, by restricting to bounded functions if necessary, we can assume in the following that this condition is satisfied.

Going back to the situation we had before, we apply the above consideration to $\Omega = \Gamma_3$ taking as V an open neighborhood of t_0. Then a formula at the end of Section 1 shows that, if $(b, a)\gamma$ is in Γ_2, A given rise to an automorphism of the lattice Γ_4 and $B(t)$ gives rise to an automorphism of the lattice $\Gamma_3(t)$. Therefore, if we take an affine coordinate system, for instance, in R so that Γ_4 becomes the lattice of integer points, A will be represented by an integer matrix.

3. The general considerations we have made so far will become exceptionally simple if we assume that

(S) <u>the center</u> G_4 <u>of</u> G_3 <u>is one-dimensional.</u>

It is the same thing to assume that R is one-dimensional over $\mathbb{R}$ or Z is one-dimensional over $\mathbb{C}$. We note that, if S is obtained from an irreducible bounded symmetric domain of type I, II, III or IV and from its highest dimensional boundary component, the condition (S) is always satisfied. A. Borel told us that the same is known also for the two exceptional cases of dimensions 16 and 27. This being remarked, if (S) is satisfied, we can identify Z with $\mathbb{C}$ so that R, C, Γ_4 are respectively identified with

$\mathbb{R}$, $\mathbb{R}^+$, $\mathbb{Z}$, Then the Fourier-Jacobi series will take the following form

$$f(z, u, t) = \sum_{k=0}^{\infty} \theta_k(u, t) e(kz) .$$

Since $\mathrm{Im}(H_t(u, v)) = [u, v]$ is non-degenerate, we have $H_t(u, u) > 0$ for $u \neq 0$. Moreover, the conditions (1), (3) in Section 1 imply that, if (A, B) comes from an element $(b, a)\gamma$ of Γ_2, we have $A = 1$ and $B(t)$ keeps H_t invariant. Therefore $B(t)$ gives rise to an automorphism of the <u>polarized abelain variety</u> $\mathcal{A}_t = U/\Gamma_3(t)$, the polarization being determined by the Riemann form $4H_t(u, v)$. In particular $\{B(t)\}$ is a <u>finite group</u> (the structure of which does not depend on t). We shall consider the simplest case assuming that

(Γ) <u>we have</u> $\Gamma_2 = \Gamma_3$.

This means precisely that we have $\{B(t)\} = 1$. In this case, if we take V sufficiently small and r sufficiently large, the quotient space

$$\mathcal{X} = \bar{S}(V, r)/\Gamma_3$$

with the ring of invariant analytic functions on $S(V, r)$ relative to Γ_3 , which is nothing else than the ring of Fourier-Jacobi series, describes the analytic structure of the compactification of S/Γ_0 around t_0 in the sense it gives a neighborhood of the image point of t_0 in the compactification together with the ring of analytic functions on it. This is because t_0 is not a fixed point of Γ_1/Γ_2 . Consider, on the other hand, an open subset W of the product $\mathbb{C} \times U \times V$ with coordinates (w, u, t) satisfying

$$\mathrm{abs}(w) < \exp(-2\pi(\mathrm{Re}(L_t(u, u)) + r)) ,$$

where abs(w) means the absolute value of w. Then (b, a) gives rise to an analytic automorphism of W as

$$(w, u, t) \longrightarrow (e(a + iL_t(2u + b(t), b(t)))w, u + b(t), t),$$

and in this way G_3 operates on W. We observe that Γ_4 is precisely the subgroup of G_3 which operates trivially on W, and Γ_3/Γ_4 operates on W properly discontinuously and without fixed points. Hence the quotient variety

$$\mathfrak{X}^* = W/(\Gamma_3/\Gamma_4) = W/\Gamma_3$$

is non-singular. We observe that invariant analytic functions in W are obtained simply by replacing e(z) by w in the Fourier-Jacobi series (of invariant analytic functions in S(V, r) both relative to Γ_3). On the other hand, we note that the closed subvariety $W_0 = (0) \times U \times V$ of $\mathbb{C} \times U \times V$ is contained in W. We shall denote its complement in W by W_1. Then both W_0 and W_1 are stable by G_3 and we have $W_1/\Gamma_3 = \mathfrak{X}^* - W_0/\Gamma_3$. More precisely, the quotient variety W_0/Γ_3 is non-singular and it is the closed subvariety of the non-singular variety $\mathfrak{X}^*$ defined by $w = 0$; the quotient variety W_1/Γ_3 is the complement of W_0/Γ_3 in $\mathfrak{X}^*$. Similarly we have $S(V, r)/\Gamma_3 = \mathfrak{X} - V$. Now we shall define a mapping $\mathfrak{X}^* \longrightarrow \mathfrak{X}$. We take a point of S(V, r) with coordinates (z, u, t) and associate the point of W_1 with the coordinates (e(z), u, t). This defines an analytic mapping $S(V, r) \longrightarrow W_1$ and, by passing to quotient varieties, it gives rise to an analytic isomorphism $S(V, r)/\Gamma_3 \simeq W_1/\Gamma_3$. Next we take a point of W_0 with coordinates (0, u, t) and associate the point t of V. This defines an analytic mapping $W_0 \longrightarrow V$ and then an analytic mapping

$W_0/\Gamma_3 \longrightarrow V$, which is surjective and proper. In fact, the fiber over an arbitrary point t of V is the abelian variety $\mathcal{A}_t = U/\Gamma_3(t)$. At any rate, if we combine the two mappings $W_1/\Gamma_3 \longrightarrow S(V, r)/\Gamma_3$ and $W_0/\Gamma_3 \longrightarrow V$, we get a continuous mapping $\mathcal{X}^* \longrightarrow \mathcal{Y}$, which is surjective and proper. The verification is left as an exercise to the reader. We know that this is an analytic isomorphism in the open subset W_1/Γ_3 . Also the remark we made before about the analytic structure of $\mathcal{X}$ around points of V shows that the mapping is analytic around points of W_0/Γ_3 . Therefore $\mathcal{X}^* \longrightarrow \mathcal{X}$ is an analytic mapping or a morphism and the theory of the theta-functions shows that it is a "blowing up" of $\mathcal{X}$ along V . We have thus obtained the following result:

THEOREM 1. Let S be a Siegel domain over T satisfying (S) ; let Γ_0 be a properly discontinuous group of analytic automorphisms of S such that T is Γ_0-rational. Then, if t_0 is not a fixed point of Γ_1/Γ_2 and if Γ_0 satisfies (Γ), a neighborhood of the image point of t_0 in the compactification of S/Γ_0 can be blown up along the image of T to a non-singular variety so that the fiber over the image point of t near t_0 is the abelian variety $\mathcal{A}_t = U/\Gamma_3(t)$.

We note that, in case Γ_0 is not small enough to satisfy (Γ) , we can still blow up the image of T so that the fiber over the image point of t is the generalized Kummer variety $U/\Gamma_2(t)$. This process was investigated by Satake [8] in the case when S is the Siegel upper-half plane and Γ_0 is the Siegel modular group of level 1 . At any rate, Theorem 1 is of fundamental importance because it gives precisely a <u>link</u> between the theory of automorphic functions and the theory of theta-functions.

4. We shall show that the said neighborhood of the image point of t_0 has no finite non-singular coverings. We shall use the same notations as before.

Let $\omega = dzdudt$ be the (highest) multiple differential form on the product $Z \times U \times T$ and consider its restriction to $S(V, r)$. Since it is invariant by Γ_3, we get a multiple differential form, which we shall also denote by ω, on the open subset $S(V,r)/\Gamma_3$ of $\mathcal{X}$. We observe that ω is holomorphic at every simple point of $\mathcal{X}$. However, since the (contravariant) image ω^* of ω under the morphism $\mathcal{X}^* \longrightarrow \mathcal{X}$ has the expression $(1/2\pi i)(dw/w)dudt$, this is not holomorphic along $w = 0$. Now, suppose that $\mathcal{X}$ has a finite non-singular covering $\mathcal{Y} \longrightarrow \mathcal{X}$. Then the image $\bar{\omega}$ of ω under $\mathcal{Y} \longrightarrow \mathcal{X}$ is holomorphic everywhere in $\mathcal{Y}$. This depends on the fact that the co-dimension of V in $\mathcal{X}$ hence also the co-dimension of the inverse image of V in $\mathcal{Y}$ are at least two. Consequently, if $\mathcal{Y}^*$ is the Oka normalization [6] of the product $\mathcal{X}^* \times_{\mathcal{X}} \mathcal{Y}$, i.e., if $\mathcal{Y}^*$ is the normalization of the graph of the "mapping" $\mathcal{Y} \longrightarrow \mathcal{X}^*$, the image $\bar{\omega}^*$ of $\bar{\omega}$ under the morphism $\mathcal{Y}^* \longrightarrow \mathcal{Y}$ is holomorphic at every simple point of $\mathcal{Y}^*$. On the other hand, since $\bar{\omega}^*$ is also the image of ω^* under the morphism $\mathcal{Y}^* \longrightarrow \mathcal{X}^*$ and since this is a covering, it is not holomorphic along the inverse image of $w = 0$. This is a contradiction. Therefore $\mathcal{X}$ has no finite non-singular coverings.

This type of argument was suggested to us by Zariski in the special case mentioned in the Introduction. We note that we can arrive at the same conclusion using either the well-known information about the total transform of a simple point or a topological mathod. We shall formulate our result in the following way:

THEOREM 2. Let S be a Siegel domain over T satisfying (S); let Γ_0 be a properly discontinuous group of analytic automorphisms of S such that T is Γ_0-rational. Then, if Γ_0 operates on S without fixed points and contains a subgroup Γ_0' of finite index satisfying (Γ), the compactification of S/Γ_0 has no finite non-singular coverings locally at any image point of T.

In fact, let t_0 be a point of T which is not a fixed point of Γ_1/Γ_2. Suppose that the compactification of S/Γ_0 has a finite non-singular covering locally at the image point of t_0. Since S/Γ_0' is unramified over S/Γ_0, this covering has to go through the compactification of S/Γ_0'. In this way [cf.5], we get a finite non-singular covering of the compactification of S/Γ_0' locally at the image point of t_0. We know, however, that this is not possible. Since points like t_0 form a dense open subset of T, the compactification of S/Γ_0 has no finite non-singular coverings at any image point of T.

We note that, in case S is obtained from a bounded symmetric domain, the existence of Γ_0' in Theorem 2 can be proved by a method which is formalized by Selberg [9]. We note also that the idea to derive Theorem 2 from Theorem 1 has been suggested to us by M. Artin. In our original formulation, Theorem 2 was stated slightly differently and was proved first (before Theorem 1) as follows. Instead of the assumption that Γ_0 contains a subgroup Γ_0' of finite index satisfying (Γ), we required that Γ_0 contains a decreasing sequence of subgroups $\Gamma_0^{(n)}$ with certain properties, which is in most cases constructible by Selberg's method, and proved that the dimensions of the Zariski tangent spaces [13] of the compactifications of $S/\Gamma_0^{(n)}$ along the images of T near t_0 tend to infinity with n. This again implies the non-existence of finite non-singular coverings of the compactification of S/Γ_0 at any image point of T. It seems that this crude method can be applied even to the case when (S) is not satisfied.

We note finally that, in some cases, we can dispense with the assumption (Γ). For instance, in the case of the compactification of the quotient variety of the Siegel upper-half plane of genus g by $Sp(g, \mathbb{Z})$, say, we can blow up the compactification along the boundary so that fibers over general points of the boundary become Kummer varieties of dimension $g - 1$. Therefore, by a similar argument as before, using $(dzdudt)^2$ instead of $dzdudt$ in the case g is even, we see that the compactification has no finite non-singular coverings locally at any boundary point for $g \geq 3$. The reason why $g = 2$ is excluded is that the Kummer variety of dimension one is exceptional. Actually, in the case $g = 2$, we have complete information since we know the structure of the compactification [4, 5]. On the other hand, if we are just interested in whether the boundary is simple or not, i.e., general points of the boundary are simple or not, we estimate the dimension of the Zariski tangent space of the compactification along the boundary. We see easily that this is equal to the number of linearly independent theta-functions of order two and of "characteristic" zero for genus $g - 1$, and it is 2^{g-1}. Since the co-dimension of the boundary is g, we get $g = 2^{g-1}$ as a necessary and sufficient condition for the boundary to be simple [cf. 13]. Hence, as it was observed recently by U. Christian [3], the boundary is singular, i.e., all boundary points are singular, for $g \geq 3$ while the boundary is simple for $g = 2$. At any rate, it is understood that, if we take a subgroup of $Sp(g, \mathbb{R})$ commensurable with $Sp(g, \mathbb{Z})$ which operates without fixed points on the Siegel upper-half plane, we can apply Theorem 2 to this subgroup as Γ_0 and we get the non-existence of finite non-singular coverings for all $g \geq 2$.

REFERENCES

1. Séminarie H. Cartan, Fonctions automorphes, E.N.S. (1957-58).

2. H. Cartan, Prolongement des espaces analytiques normaux, Math. Ann., 136 (1958), pp. 97 - 110.

3. U. Christian, Zur Theorie der Hilbert-Siegelschen Modulfunktionen Math. Ann., 152 (1963), pp. 275-341.

4. J. Igusa, On Siegel modular forms of genus two, Amer. J. Math., 84 (1962), pp. 175 - 200.

5. ______, On Siegel modular forms of genus two (II), to appear in the Americal Journal of Mathematics, 86 (1964).

6. K. Oka, Sur les fonctions analytiques de plusieurs variables VIII, lemme fondamental, J. Math. Soc. Japan, 3 (1951), pp. 204 - 214, 259-278.

7. P. Samuel, Travaux d'Igusa sur les formes modulaires de genre 2, Seminaire Bourbaki (1963-64), n°267.

8. I. Satake, On Siegel's modular functions, Proceedings of the International Symposium on algebraic number theory, Tokyo-Nikko (1955), pp. 107-129.

9. A. Selberg, On discontinuous groups in higher-dimensional symmetric spaces, Contributions to function Theory, Tate Institute of Fundamental Research, Bombay (1960), pp. 147 - 164.

10. I.I. Pyatetski-Shapiro, The geometry of classical domains and the theory of automorphic functions, Moscow (1961).

11. C.L. Siegel, Analytic functions of several complex variables, I.A.S., (1948 - 49).

12. A. Weil, Introduction à l'études des variétés kähleriennes, Actualités Scientifiques et Industrielles, Paris (1958).

13. O. Zariski, The concept of a simple point of an abstract algebraic variety, Trans. Amer. Math. Soc., 62 (1947) pp. 1 - 52.

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 $X' \to X$. A family of maps $\{X'_i \to X'\}$ over X is called a covering if X' is set theoretically the union of the images of the X_i's.

Let us suppose that $f : X' \to X$ 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"

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

and the following result holds.

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

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

induced by ε are isomorphisms for each q.

This theorem in its general form requires resolution of singularities. The étale cohomology theory does <u>not</u> 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.

Base should be connected

<u>Theorem</u>: 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.

<u>Elementary Theory</u>:

<u>Case X = Spec k, k a field</u>: 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].

<u>Kummer Theory</u>: 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

<u>Hilbert Theorem 90</u>: $H^1(X, (\mathbb{G}_m)_X) = \operatorname{Pic} X$ 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 nth 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 nth power. One has therefore an exact sequence.

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

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

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

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

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

$$\begin{tikzcd} 0 \arrow[r] & \mu_n \arrow[r] & \Gamma(X,\mathcal{O}_X)^* \arrow[r, "n"] & \Gamma(X,\mathcal{O}_X)^* \arrow[r] & H^1(X,\mu_n) \arrow[r] & \operatorname{Pic} X \arrow[d, "n"] \\ & & & .0 & H^2(X,\mu_n) \arrow[l] & \operatorname{Pic} X \arrow[l] \end{tikzcd}$$

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

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

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 μ_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 $\bar{y}$ be a geometric point of Y, and let $X_{\bar{y}}$ be the fibre of X/Y at $\bar{y}$. Then the stalk

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

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 $\bar{y}$ is the closed point of Y. Then the stalk of $R^q f_* F$ at $\bar{y}$ 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 $\leqq 1$ (in fact to the case $X = \mathbb{P}^1_Y$ if one wants). The case of relative dimension $\leqq 1$ 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 <u>surjectivity</u> for $q > 0$. That is an elementary exercise on morphisms of δ-functors. Remember that we are in the case of relative dimension $\leqq 1$, i.e., in the case X_0 is an algebraic scheme of dimension $\leqq 1$. 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

<u>Lemma</u>: Let X be noetherian and F a noetherian torsion sheaf on X. There is an integer N, a collection of <u>finite</u> 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

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

<u>bijective</u> if $q = 0$ and <u>surjective</u> 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 μ_n and apply Kummer Theory. One finds a diagram

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

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

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

surjective. Again using Hensel's Lemma and the fact that $\dim X_0 \leq 1$, 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:

$$\begin{tikzcd} X & X' \arrow[l, "g'"'] \arrow[d, "f'"] \\ S \arrow[from=u, "f"'] & S' \arrow[l, "g"] \end{tikzcd}$$

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-imersion 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 δ-functor. It can be shown that it is in general not a derived functor.

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

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

Proof: 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:

$$\begin{tikzcd}
 & X' \arrow[dr, "g"] \arrow[dd, "f'"'] & \\
X \arrow[ur, "i"] \arrow[rr, "i'"'] & & X'' \arrow[dl, "f''"] \\
 & S &
\end{tikzcd}$$

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:

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

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_σ the prescheme $U_{\alpha_1} \times_S \cdots \times_S U_{\alpha_p}$ and by f_{U_σ} the morphism f composed with the canonical morphism $U_\sigma \longrightarrow X$. Let us denote by F/U_σ the inverse image of the sheaf F on U_σ. 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

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

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:

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

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

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

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_σ and extended by zero. The complex of sheaves on X: $C^*(U_\alpha, F)$ deduced from the semi-simplicial complex

$$\begin{matrix}\rightrightarrows\\ \rightarrow\end{matrix} \coprod_{\alpha,\beta} F_{U_\alpha \times_S U_\beta !} \rightrightarrows \coprod_{\alpha} F_{U_\alpha !} \longrightarrow F$$

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 μ_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 : μ_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

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

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

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

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:

TR 0) $\rho_{X,S}(F)$ is functorial in F.

TR 1) $\rho_{X,S}$ is compatible with the change of the base.

TR 2) $\rho_{X,S}$ is compatible with the composition of the morphisms.

TR 3) 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 ω_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 η_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 α that we can include in a diagram :

$$(3.1.1)\qquad \begin{array}{ccc} R^{2(d+d')} gf_!(T_{X/S} \otimes f^*g^*F) & \xrightarrow[\alpha]{\sim} & R^{2d'} g_! R^{2d} f_!(T_{X/S} \otimes f^*(T_{S/Y} \otimes g^*F)) \\ \downarrow{\scriptstyle \rho_{X,Y}} & & \downarrow{\scriptstyle R^{2d'} g_!(\rho_{X,S})} \\ F & \xleftarrow{\rho_{Y/S}} & R^{2d'} g_!(T_{S/Y} \otimes g^*F) \end{array}$$

The axiom (TR 2) is that the above diagram must be commutative.

Proof of the proposition: Uniqueness: By (TR 1) we are reduced to the case $S = \mathrm{spec}(k)$ where k is an algebraically closed field. By (TR 2), (TR 3) and the exact sequence (2.2.1) we are reduced to the case when X is affine and f of the type:

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

where g is étale and $\underline{A}_k^d$ is the affine space of dimension d over k (Definition of smooth morphism). By (TR 3) and (TR 2) we are reduced to the case $X = \underline{A}_k^d$ and $f : \underline{A}_k^d \longrightarrow \mathrm{spec}(k)$ the canonical morphism. By induction on d and (TR 2) we are reduced to the case $f : \underline{A}_k^1 \longrightarrow \mathrm{spec}(k)$. Since the functors $R^q f_!$ commute with inductive limits we can suppose that $F = \underline{Z}/n$. The axiom (TR 4) 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 $X \xrightarrow{g} \underline{A}_S^d \longrightarrow S$ with g étale and that it satisfies (TR i), $0 \leq i \leq 4$. Then, by localization on X (2.2.1) and on S, we can construct it in the general case. The properties (TR i), $0 \leq i \leq 4$, 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 (TR 1) and (TR 2) 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:

$$\begin{tikzcd} X \arrow[r, "g'"] \arrow[d, "g"'] & \underline{A}^1_k \arrow[d, "h'"] \\ \underline{A}^1_k \arrow[r, "h'"] & S = \mathrm{spec}(k) \end{tikzcd}$$

with g and g' étale and h and h' canonical, the two morphisms $R^2f_!(T_{X/S}) \rightrightarrows \underline{Z}/n$ 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 (TRi) can be easily deduced afterward. To show this independence, we can suppose that $S = \mathrm{spec}(k)$ (algebraically closed field). Let us consider

$$\begin{tikzcd} X \arrow[r, "g"] \arrow[d, "g'"'] & \underline{A}^d_S \arrow[d] \\ \underline{A}^d_S \arrow[r] & S = \mathrm{spec}(k) \end{tikzcd}$$

two factorizations of f. An S-morphism of X into an affine space over S is determined by d global sections of O_X : $\eta_1, \eta_2, \dots \eta_d$. 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 O_X. Let $d\eta_1 \dots d\eta_d$ be the differentials of the sections $\eta_1 \dots \eta_d$. 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 $\eta'_1, \dots \eta'_d$ be d sections of O_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:

$$\begin{tikzcd} X \arrow[r] \arrow[d, "g'"'] & \underline{A}^1 \underline{A}^{d-1}_S \arrow[d] \\ \underline{A}^1 \underline{A}^{d-1}_S \arrow[r] & \underline{A}^{d-1}_S \end{tikzcd} \qquad S = \mathrm{spec}(k).$$

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 $X = P^1_S$. But in this case the sheaf on S :

$R^1 f_!(G_m)$ 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 $S = \mathrm{spec}(k)$ (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 $F^\bullet$ 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 $F^\bullet$ of $D_n(X)$ whose objects $(F^\bullet)^\ell$ are null for $\ell < \ell^0(F^\bullet)$ (resp. $\ell > \ell^0(F^\bullet)$, resp. $\ell^0(F^\bullet) < \ell$ and $\ell < \ell^1(F^\bullet)$).

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

$$\deg(w) = 1 \qquad \begin{tikzcd} & H^\bullet \arrow[dl, "w"'] \arrow[dr, "v"] & \\ F^\bullet \arrow[rr, "u"] & & G^\bullet \end{tikzcd} \qquad (*)$$

Such triangles are called the <u>distinguished triangles.</u>

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

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

$$\dots \longrightarrow R^0F^\bullet \longrightarrow R^0G^\bullet \longrightarrow R^0H^\bullet \longrightarrow R^1F^\bullet \longrightarrow \dots$$

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

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

The category $D_n^+(X)$ is equivalent to the category of complexes of injective sheaves, bounded below, up to homotopy. A <u>resolution</u> $F^\bullet \longrightarrow G^\bullet$ of a complex $F^\bullet$ 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 yeild functorially distinguished triangles.

4.2. <u>The exact functor $Rf_!$.</u>

Let $X \xrightarrow{i} X' \xrightarrow{f} S$ be an S-imersion of X into a projective prescheme over S. Let $F^{\bullet}$ be a complex of sheaves on X bounded below and let us take a resolution of $i_! F^{\bullet}$ 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 $\underline{R}f_!(F^{\bullet})$. It can be shown that the object $\underline{R}f_!(F^{\bullet})$ depends functorially on $F^{\bullet}$, (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:

$$\begin{tikzcd} X \arrow[d, "f"'] & X' \arrow[l, "u"'] \arrow[d, "f'"] \\ S & S' \arrow[l, "u'"] \end{tikzcd}$$

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. <u>**The twisted inverse image functor.**</u>

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** $f^{!}(G^{\cdot})$ **the following complex of sheaves on** X **:**

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

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

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:**

$$\begin{tikzcd} X & X' \arrow[l, "u"'] \arrow[d, "f'"] \\ S \arrow[from=u, "f"'] & S' \arrow[l, "u'"] \end{tikzcd}$$

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 $i_! f^!(G)$:

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

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

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

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:

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

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 $K^{\bullet}$ be an object of $D^{+}_{n}(X)$ and $H^{\bullet}$ be an object of $D_{n}(X)$. Let us denote by $\underline{\mathrm{RHom}}(H^{\bullet}, K^{\bullet})$, the following complex on X : Take an injective resolution $I^{\bullet}$ of the complex $K^{\bullet}$ and consider the object of $D_{n}(X)$ defined by the complex of sheaves: $\underline{\mathrm{Hom}}^{*}(H^{\bullet}, I^{\bullet})$ where $\underline{\mathrm{Hom}}$ is the homomorphism sheaf. Let us assume now that $H^{\bullet}$ 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 : $\underline{\mathrm{R}}\mathrm{Hom}(H^{\bullet}, K^{\bullet})$. The sheaves of cohomology of $\underline{\mathrm{RHom}}(H^{\bullet}, K^{\bullet})$ are the local hyper-ext. The groups of cohomology of $\underline{\mathrm{R}}\mathrm{Hom}(H^{\bullet}, K^{\bullet})$ are the global hyper-ext.

In the same way we define $\underline{\mathrm{R}}f_{*}(K^{\bullet})$: Take an injective resolution and apply the direct image functor.

By functoriality of $\mathrm{R}f_{!}$, for any $H^{\bullet}$ object of $D^{-}_{n}(X)$ and $K^{\bullet}$ object of $D^{+}_{n}(X)$, we get a functorial morphism:

$$\underline{\mathrm{R}}f_{*}\underline{\mathrm{RHom}}(H^{\bullet}, K^{\bullet}) \longrightarrow \underline{\mathrm{RHom}}(\mathrm{R}f_{!}(H^{\bullet}), \mathrm{R}f_{!}(K^{\bullet}))$$

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

$$\underline{\mathrm{R}}\mathrm{Hom}(H^{\bullet}, K^{\bullet}) \longrightarrow \underline{\mathrm{R}}\mathrm{Hom}(\underline{\mathrm{R}}f_{!}(H^{\bullet}), \underline{\mathrm{R}}f_{!}(K^{\bullet}))$$

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

$$\mathrm{Ext}^{p}(H^{\bullet}, K^{\bullet}) \longrightarrow \mathrm{Ext}^{p}(\underline{\mathrm{R}}f_{!}(H^{\bullet}), \underline{\mathrm{R}}f_{!}(K^{\bullet}))$$

But now using the trace morphism, we obtain morphisms:

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

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

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

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 $S = \mathrm{spec}(k)$ (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 $R^p f_!(F)$):

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

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

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

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 $\triangle^i_{X/S}$ is always an isomorphism, all the $\triangle^i_{X/S}$ 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), $F^{\bullet}$ be an object of $D^-_n(X)$ and $G^{\bullet}$ be an object of $D^+_n(S)$. We shall denote by $(i, X, S, F^{\bullet}, G^{\bullet})$ the property: The morphism $\triangle^i_{X/S}(F^{\bullet}, G^{\bullet})$ 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 $(i, X, S, \underline{Z}/n_{U!}, G)$.

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), $H^\bullet$ 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:

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

Then the third one also holds.

<u>Proof:</u> 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 $F^\bullet$ of $D_n^-(X)$ admits a resolution $P^\bullet \longrightarrow F^\bullet$ by a complex of the type : $P^\bullet = \ldots \longrightarrow \underline{Z}/n_{U_i!} \longrightarrow \underline{Z}/n_{U_k!} \longrightarrow 0 \longrightarrow \ldots$ 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 $F^\bullet = \coprod_i \underline{Z}/n_{U_i!}$, 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 $F^\bullet = \underline{Z}/n_{U_i!}$. Again by spectral sequence argument we can suppose that $G^\bullet = G$ 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 $\mathrm{Ext}^*(\underline{R}f_!(\underline{Z}/n_{U_i!}), G)$ and $\mathrm{Ext}^*(\underline{Z}/n_{U_i!}, f^! G)$ 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 <u>First reduction:</u> 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 $F^\bullet$ is the constant sheaf $\underline{Z}/n$.

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

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

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

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 η (they are constructible). Therefore the cohomology sheaves of the complex $\underline{\mathrm{RHom}}(\underline{R}f_!(\underline{Z}/n), G)$ are constant on an étale neighborhood of η.

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 η. 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 η, it is enough to look at the fiber $X_{\bar{\eta}} \longrightarrow \bar{\eta}$, i.e., we are reduced to the case $S = \mathrm{spec}(k)$ (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 $S = \mathrm{spec}(k)$ (algebraically closed field).

Let us suppose that $S = \mathrm{spec}(k)$, 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 $F^{\bullet}$ is the constant sheaf $\underline{Z}/n$.

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

Thus we have to prove that the morphisms:

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

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

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

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 COHOMOLCGY CLASSES

J. Tate

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

$$
\begin{tikzcd}
 & \overline{V} = V \times_k \overline{k} \arrow[dl, dash] \arrow[dr, dash] & \\
V \arrow[dr, dash] & & \overline{k} \arrow[dl, dash, "G(\overline{k}/k)"] \\
 & k &
\end{tikzcd}
$$

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

$\overline{V} = V \times_k \overline{k}$ the scheme obtained from V by base extension to $\overline{k}$. For each prime number ℓ different from the characteristic of k, we put

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

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

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

In the abstract case there is no good cohomology with rational coefficients, and it is the groups $H^i_\ell(\overline{V})$ 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_ℓ. The proper base change theorem shows that the groups H^i_ℓ do not change if we replace $\overline{k}$ 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 $G(\overline{k}/k)$ operates on the groups $H^i_\ell(\overline{V})$. Namely, it operates on the product $\overline{V} = V \times_k \overline{k}$ through the second factor, and hence on the site $\overline{V}_{\text{étale}}$; the point is that the étale topology depends only on $\overline{V}$ and not on the arrow $\overline{V} \longrightarrow \operatorname{Spec} \overline{k}$ which is used to define the classical topology when $\overline{k} = \mathbb{C}$.

There results a homomorphism

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

(where $b_i = \dim_{\mathbb{Q}_\ell} H^i_\ell = i^{th}$ 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_ℓ of $\mathbb{GL}(b_i, \mathbb{Q}_\ell)$. 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_ℓ is an ℓ-adic Lie group, whose Lie algebra $\mathfrak{g}^i$ 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 peehaps 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 k and V, and depend only on</u> $X/\mathbb{C}$. Almost nothing is known about them, cf. Serre [4]. Is their dimension and type independent of ℓ? 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 $x \in \mathcal{U}_\ell^{2i}$, 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 θ is the class of an algebraic cycle of codimension i if and only if $x\theta = \lambda_i(x)\theta$ for all $x \in \mathcal{U}_\ell^{2i}$.

§ 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

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

is the one dimensional ℓ-adic vector space on which $G(\bar{k}/k)$ operates according to its action on the group μ_{ℓ^n} of ℓ^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

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

(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 $H_\ell^i(\bar{V})$, then we replace $H_\ell^i(\bar{V})$ by its m-fold twisting $H_\ell^i(\bar{V})(m)$.

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

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

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

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

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 $\eta \in H^{2(d-1)}(\bar{V})(d-i)$. Extending c by additivity we obtain in this way a homomorphism

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

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 $\mathcal{Z}_h^i(\bar{V})$ 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 "ℓ-adically homologically equivalent to zero") and put

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

One has the following conjectural statements.

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

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

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

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

is injective.

Statements (a) and (b) are true in characteristic zero, because we can then imbed k in $\mathbb{C}$ and factor the map α 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 .

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

where δ_n is the connecting homomorphism in the cohomology sequence derived from the exact sequence

$$(6) \qquad 0 \longrightarrow \mu_{\ell^n} \longrightarrow \mathbb{G}_m \xrightarrow{\ell^n} \mathbb{G}_m \longrightarrow 0$$

(see the talk of Mike Artin). For each n the kernel of δ_n is $\ell^n H^1(\bar{V}_{\acute{e}t}, \mathbb{G}_m)$, 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 $\overline{V}$ is "defined" over a finite extension of k. Thus X is fixed by an open subgroup U of $G(\overline{k}/k)$, 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 $c(\mathcal{A}^i(\overline{V}))\mathbb{Q}_\ell$ consists of those elements of $H^{2i}_\ell(\overline{V})(i)$ whose stabilizer is open in $G(\overline{k}/k)$, that is, which are annihilated by the corresponding Lie algebra.

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

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

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

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

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

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

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

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

where $A(\ell^\infty)$ denotes the $G(\bar{k}/k)$-module of points on A of order ℓ^ν, all ν, with coefficients in $\bar{k}$. 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 ψ_N coincides with φ on the points of order ℓ^N.

Mumford has verified (8) in case k is finite and A and B are of dimension 1, by lifting the Frobenius endomorphism to charactertistic 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 $c \in c(\mathcal{Q}^{i})\mathbb{Q}_{\ell}$ then $c_{a,b} \in c(\mathcal{Q}^{i})\mathbb{Q}_{\ell}$ for all a, b. Grothendieck conjectures that the same is true with $\mathbb{Q}$ instead of $\mathbb{Q}_{\ell}$, 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 φ. Then the algebraic number $\Lambda(\varphi)$ of fixed points of φ is given by the Lefschetz formula

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

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 ℓ .

(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 weite

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

with complex α_{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 φ 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 σ 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 σ as element of $G(\bar{k}/k)$.

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

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

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 ζ; see Weil [9]. Since the "reciprocal roots" α_{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 σ operates as q on our twisting space, W, because σ raises ℓ^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

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

assuming, as always, that (a), (b), (c), and (d) hold. Moreover, the inequality $\leq$ 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

$$\text{(13)} \qquad X_0^n + X_1^n + \dots + X_r^n = 0$$

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 $\mathcal{A}^i(V)$ 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 ν, 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

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

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 $H_\ell^{2i}(\bar{V})$ 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 $\mathcal{Q}^1$ 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 $V \longrightarrow (\operatorname{Spec} k)$. (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 $0 \leq i \leq 2d$,

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

The $P_{y,i}(t)$ are of fixed degree (see below) with reciprocal roots α_{ij} of absolute value $(Ny)^{1/2}$ (recall that we <u>assume</u> conjecture (d) of § 3). Therefore, by theorem 1 of Serre's talk the product (16) converges absolutely for $Rs > \dim Y + \frac{i}{2}$. It is conjectured that the Φ_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 $Rs > \dim Y + \frac{i}{2} - 1$. It follows that (insofar as Φ_i is extendible there) the zeros and poles of Φ_i in the strip

$$\dim Y + \frac{i}{2} - 1 < Rs \leq \dim Y + \frac{i}{2}$$

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 Φ_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 $\mathcal{Q}^i(V)$ 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 $s = \dim X - 1$ 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

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

and let

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

Then we have

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

where

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

for $\nu > 0$.

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

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

$$\text{(19)} \qquad \operatorname{rank} \mathcal{Q}^i(V) = \operatorname{rank} \mathcal{Q}^i(\bar{V}) = \binom{m}{i}^2 - \binom{m}{i-1}\binom{m}{i+1} \quad .$$

Let c_ν 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 formally 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 ν 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 $\mathcal{Q}^i(E^m)$ 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 ℓ-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 $H^i_\ell(\overline{V}_y)$ are independent of y for $y \in Y_\ell$ (here the Y_ℓ denotes the locus $\ell \neq 0$ in Y). To make the statement precise, one chooses a "strict localization" $\overline{O}_y \subset k$ of the local ring O_y of y on Y, and uses the residue field of $\overline{O}_y$ as the algebraic closure $\overline{k(y)}$ of k(y). The decomposition subgroup $D_y = \{\sigma \in G(\overline{k}/k) | \sigma\overline{O}_y = \overline{O}_y\}$ 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 $\overline{O}_y$, which plays the role of a path from the general geometric point, spec $\overline{k}$, to the special one, spec $\overline{k(y)}$. This "path" determines an isomorphism

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

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

For each closed $y \in Y_\ell$, let σ_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, σ_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 $H^i_\ell(\bar{V})$ as φ_y does (see p. 11), shows that the polynomial $P_{y,i}(t)$ in (16) is given by

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

where $\sigma_{y,i,\ell}$ denotes the endomorphism of $H^i_\ell(\bar{V})$ induced by the operation of σ_y. Thus, <u>the function</u> Φ_i <u>is completely determined by the scheme</u> Y, <u>together with the</u> ℓ <u>-adic representations</u> $H^i_\ell(\bar{V})$ <u>of the fundamental groups</u> $\pi_1(Y_\ell)$. 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 $\ell \neq \operatorname{char} k$ we have a finite dimensional vector space H_ℓ over $\mathbb{Q}_\ell$ on which $\pi_1(Y_\ell)$ operates continuously in such a way that the characteristic polynomial

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

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

Given such a system, we put

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

this product being absolutely convergent for $Rs > \rho + \dim Y$. 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

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

is an L-series for the system of representations $(H^i_\ell(\overline{V}))$ 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:

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

Thus

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

belongs to the representation system $H^{2i}(\overline{V})(i)$ 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 $H^{2i}(\overline{V})(i)$ which is fixed under $\pi_1(Y)$. If we assume the $\pi_1(Y_\ell)$-modules $H^i_\ell(\overline{V})$ 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 $H = (H_\ell^{2i}(\overline{V})(i))$, 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_ℓ (this being independent of ℓ).

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 $\overline{V}$ 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 $\mathbb{Z}$ 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 $f\colon X \longrightarrow Y$ 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 $\mathbb{Z}$, 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 ℓ-adiques attaches aux courbes elliptiques, colloque de Clermont-Ferrand, April, 1964.

[6] Taniyama, Y., $\mathcal{L}$-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 μ 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 μ 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 $\underline{X} + (-y)$. 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, μ) and (D', μ') are in the same class if there is a birational equivalence over k which takes D into D' and μ into μ' (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 $H^1(\Gamma, \overline{\mathfrak{g}})$, where Γ is the Galois group of the algebraic closure $\bar{k}$ of k over k and $\overline{\mathfrak{g}}$ is the group of points on $(C, \underline{o})$ defined over $\bar{k}$. 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.,

$$H^1(\Gamma, \overline{\mathfrak{g}}) = \varinjlim_{K} H^1(\Gamma_{k/K}, \mathfrak{g}_K),$$

where K runs through all finite normal extensions of k. If (D, μ) is any homogeneous space the corresponding element of $H^1(\Gamma, \overline{\mathfrak{g}})$ is given by the cocycle $\sigma \mathfrak{a} - \mathfrak{a} = \mathfrak{a}_\sigma \in \overline{\mathfrak{g}}$ $(\sigma \in \Gamma)$ where $\mathfrak{a}$ is any point on D defined over $\bar{k}$ and the subtraction is that given by the structure μ of homogeneous space. The group law on $\overline{\mathfrak{g}}$ gives a group law on $H^1(\Gamma, \overline{\mathfrak{g}})$ 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 Proofs of the conjectures seem, however, to be as far away as ever. In describing 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 $\mathfrak{G}_v$ the group of points defined over k_v, endowed with the v-adic topology. Then $\mathfrak{G}_v$ is compact because C is complete. It is natural to define an adele to be just an element of the compact group $\prod_v \mathfrak{G}_v$ (with the product topology). There is a natural injection

$$\mathfrak{G} \longrightarrow \prod_v \mathfrak{G}_v$$

of the group $\mathfrak{G}$ of points defined over k into the adele group: the points of the image are the principal adeles. 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 $\mathfrak{G}$ is finite.

Let ω 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 ω gives a normalization of the Haar measure on $\mathfrak{G}_v$ 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 0_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 additive group k_v, appropriately normalized. The normalization is

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

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 $\mathfrak{G}_v$. 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

$$m_v(\mathfrak{G}_v) = \frac{N_v}{\mathcal{N}(v)} \tag{2}$$

with the above choice of ω, where N_v is the number of points on the reduced curve and $\mathcal{N}(v)$ is the number of elements of the residue class field. For the remaining finitely many non-archimedean valuations $m_v(\mathfrak{G}_v)$ is a rational number which can, in any individual case, be found after a trivial, if sometimes tedious, computation; and v for archimedean $m_v(\mathfrak{G}_v)$ is readily expressed in terms of the periods of ω (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 ω of the first kind. If ω' is another such differential, then $\omega' = \lambda\omega$ for some $\lambda \in k$ and so

$$m_v'(\ ) = |\lambda|_v\, m_v(\ ),$$

where m_v' is defined in terms of ω' as m_v is in terms of ω. Hence

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

if the product converges, is independent of the choice of ω 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

$$\tau = \frac{\#(Ш)}{\{\#(\mathfrak{g})\}^2}, \tag{4}$$

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 $\#(\mathfrak{g})$ is infinite.

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

$$\prod_{v \text{ "good"}} \frac{N_v}{\mathfrak{N}(v)} \tag{5}$$

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:

$$\zeta_v(s) = \frac{f_v(s)}{\{1-(\mathfrak{N}(v))^s\}\{1-(\mathfrak{N}(v))^{1-s}\}}$$

where

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

$$f_v(1) = n_v/\mathfrak{N}(v). \tag{6}$$

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 Grössencharaktere. (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 ℓ is a certain function defined on the curve $y^2 = 4x^3 - 4x$, ϑ runs through the group Δ of all D-division points on this curve and χ is a character on Δ. Application of Galois theory to this formula shows that τ 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 τ for a large number of values of D and also to find $\mathfrak{G}$. (As I explained in my Stockholm Oration there is no sure-fire algorithm for finding $\mathfrak{G}$ but experience shows that it can usually be done.) They found the following experimental facts, both in accordance with the conjecture (4):

(i) $\tau = 0$ if and only if $\#(\mathfrak{G}) = \infty$

(ii) τ 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 τ obtained agree with what is known about Ш. (This is precious little except for the 2- and 3-components. Some of the values of τ 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

$$m_v(\mathfrak{G}_{1v}) = \frac{N_{1v}}{\mathfrak{N}(v)} = \frac{N_{2v}}{\mathfrak{N}(v)} = m_v(\mathfrak{G}_{2v})$$

for all except a finite number of v and so that

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

is well defined. It can be shown that

$$T(C_1/C_2) = \frac{\#\{\mathfrak{G}_2/v_1\mathfrak{G}_1\}\#\{(\mathfrak{G}_2)_{v_2}\}\#\{(Ш_1)_{v_1}\}}{\#\{\mathfrak{G}_1/v_2\mathfrak{G}_2\}\#\{(\mathfrak{G}_1)_{v_1}\}\#\{(Ш_2)_{v_2}\}} \tag{11}$$

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

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 $\mathfrak{g}$ 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

$$\#\{(Ш_1)_{v_1}\} = \#\{Ш_1/v_2Ш_2\}$$

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 $\#(\mathfrak{g})^2$ 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 $\#(\mathfrak{g})$. 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 $\mathfrak{g}$. (The finite generation of $\mathfrak{g}$ 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 $\mathfrak{G}$, 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 parity of the order of the zero of $L(s)$ at $s = 1$ from the functionsl 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 parity of g under the conjecture that Ш_1, 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 typical 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 $\prod(1-\alpha_i t)/\prod(1-\beta_j t) = 1 + c_1 t + c_2 t^2 + \ldots$ where the α_i and β_j are finite in number and are algebraic numbers while $c_1, c_2, \ldots$ 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 α_i^{-1} nor β_j^{-1} can have p-adic value strictly less than 1 and thus each α_i and β_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 ggain 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 $\operatorname{ord} x > -(p-1)/p$ 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 π is replaced by π' where $|\pi - \pi'| < 1$.

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

Let Ω be the completion of the algebraic closure of the p-adic rationals. Let $f(\dot{x})$ be a homogeneous polynomial of degree d in $\dot{x} = (x_1, \ldots, x_{n+1})$ with coefficients in the ring of integers of Ω 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 $x_{i_1} = x_{i_2} = \cdots = x_{i_r} = 0$ 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 $dw_0 = w_1 + \cdots + w_{n+1}$. Let K be the space of elements, ξ^*, in $\mathcal{L}^*$ such that

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

where $E_i = x_i \dfrac{\partial}{\partial x_i}$, $f_i = E_i f$ and γ_- 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 position 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

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

of K , where Φ 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 α^* is "essentially" $\exp(-\pi x_0 f(x)) \circ \Phi \circ \exp(\pi x_0 f(x))$.

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, $f(x, \Gamma)$, of hypersurfaces of degree d in $x_1, \ldots, x_{n+1}$ parametrized by a new indeterminate, Γ. As before we construct K_Γ but here the elements lie in $\Omega(\Gamma)[[\frac{1}{x_0}, \frac{1}{x_1}, \ldots, \frac{1}{x_{n+1}}]]$. Let $R(\Gamma)$ be the resultant of $E_1 f(x, \Gamma), \ldots, E_{n+1} f(x, \Gamma)$, viewed as polynomials in $x_1, \ldots, x_{n+1}$. We construct a basis of K_Γ of the form

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

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 Γ close to zero, (we now dedefine K_Γ 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_Γ (we suppose $R(0) \neq 0$) ; relative to our bases this mapping has matrix C_Γ which satisfies a system of ordinary linear differential equations with rational coefficients and we obtain the commutative diagram

$$\begin{array}{ccc} K_0 & \longrightarrow & K_{\Gamma^q} \\ \alpha_0^* \downarrow & & \downarrow \alpha_\Gamma^* \\ K_0 & \longrightarrow & K_\Gamma \end{array}$$

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

Writing this in matrix form

$$\alpha_\Gamma^* = C_{\Gamma^q}^{-1}\, \alpha_0^*\, C_\Gamma$$

and α_Γ^* 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_Γ^s denote the elements, ξ^*, of K_Γ which have the property that no single monomial $\dfrac{1}{x^w}$ occurring in ξ^* 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 $f(x,\Gamma) \equiv 0$ where Γ 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 $C_\Gamma^t JC_\Gamma$ is a rational matrix function of Γ, J being a suitable constant nonsingular matrix.

For elliptic curves, C_Γ 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_Γ (as transformation of $\overline{K}_0$ onto $\overline{K}_\Gamma$) 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 Γ for Γ 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_Γ be the Vandemonde matrix

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

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

The interpretation of the matrix of α_Γ^* relative to our basis in the zero dimensional case should be of some interest. If Γ is specialized so that $\Gamma^q = \Gamma$ and $\overline{f}$ has coefficients in the field of q elements then α_Γ^* 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 $\mathbb{Z}$, then the construction of the basis of K_Γ is independent of p and it seems possible that if Γ_0 is a fixed element of $\mathbb{Z}$ and if for each prime p (excluding primes which divide $R(\Gamma_0)$, in this case the discriminant), we specialize Γ so that $\Gamma \equiv \Gamma_0 \bmod p$, $\Gamma^q = \Gamma$, then the matrices α_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 α^*_Γ 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

$$0 \longrightarrow \mathcal{L}^* \longrightarrow \mathcal{L}^{*\,(n+1)}_{\;1} \longrightarrow \mathcal{L}^{*\,(n+1)}_{\;1} \longrightarrow \ldots$$

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

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

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, α^* 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 α^* 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 extablishing 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

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

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: <u>For every</u> i, $\zeta^{(i)}(s; V/k)$ <u>is meromorphically continued on the whole</u> s-<u>plane and satisfies a functional equation.</u> 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 ℓ-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 $\mathrm{End}_{Q}(V)$ is isomorphic to an algebraic number field F of degree $2n$.[1]

---

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

It can be shown that there exists an element $\mu_{\mathfrak{p}}$ in $\mathrm{End}_{Q}(V)$ whose reduction modulo $\mathfrak{p}$ is $\pi_{\mathfrak{p}}$. Moreover, one can determine the prime ideal-decomposition of $(\mu_{\mathfrak{p}})$ in F. These facts, together with a simple class-field theoretical consideration, show that $\mathfrak{p} \rightarrow \mu_{\mathfrak{p}}$ 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 $\pi_{\mathfrak{p}}$ can be lifted up to an element of $\mathrm{End}_{Q}(V)$ for every $\mathfrak{p}$. Of course we can not expect this in general. However, in the case (II), we can show, roughly speaking, that $\pi_{\mathfrak{p}} + \pi_{\mathfrak{p}}{}^*$ 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 Γ of $SL_2(R)$ is called a Fuchsian group of the first kind, if H/Γ is of finite measure. Hereafter we fix such a Γ. An element

$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of Γ, other than ± 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 Γ. Let s be a cusp of Γ. All the elements of Γ which leave s invariant are parabolic. Together with ± 1, they form a group which is the product of $\{\pm 1\}$ and an infinite cyclic group generated by an element τ of the form $\tau = \rho \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rho^{-1}$ with an element ρ of $SL_2(R)$ such that $\rho(\infty) = s$. Let H^* be the union of H and all the cusps of Γ. We can introduce a complex structure H^*/Γ so that H^*/Γ 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 Γ. Therefore H/Γ is compact if and only if Γ 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> Γ is a meromorphic function f on H satisfying the following conditions (A1, 2).

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

To describe the condition (A2), take a cusp s of Γ and elements τ, ρ 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 $f(\rho(z))\, j(\rho, z)^m = F_s(e^{2\pi}$
Then (A2) is stated as follows:

(A2) For every cusp s of Γ, $F_s(q)$ 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^*/Γ and φ is a natural projection of H^* to H^*/Γ, then $g \circ \varphi$ is an automorphic function with respect to Γ; conversely, every automorphic function with respect to Γ 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 Γ, $F_s(q)$ is holomorphic at $q = 0$.

We denote by $S_m(\Gamma)$ the set of all cusp forms of weight m with respect to Γ. The dimension of $S_m(\Gamma)$ can be determined easily by means of the Riemann-Roch theorem for H^*/Γ. 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^*/Γ, defined by $\omega \circ \varphi = f(z)\,dz$. Therefore the dimension of $S_2(\Gamma)$ over C is exactly the genus of H^*/Γ.

3. Hecke operators. Let Δ be the subset of $GL_2(R)$, closed under multiplication, and containing Γ. 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 Γ.

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

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 $g = f \mid T_m(\Gamma\alpha\Gamma)$ 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 Γ is $SL_2(Z)$, and Δ 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 represen tatives 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 α, let $T(a, d)$ denote $\Gamma\alpha\Gamma$ (as an element of $R(\Gamma, \Delta)$). Then we have

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

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

$\lambda + \mu = n$, $\mu \geqq \lambda \geqq 0$. 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,

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

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

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

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:

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

Let us define <u>the principal congruence subgroup</u> Γ_N <u>of level</u> N by

$$(3.5) \qquad \Gamma_N = \{\alpha \in SL_2(Z) \mid \alpha \equiv 1 \bmod (N)\},$$

for every positive integer N. An automorphic form (resp. function) with respect to Γ_N is usually called a <u>modular form</u> (resp. <u>function</u>) <u>of level</u> N. Let Δ_N be the set of all matrices α in Δ 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 α in Δ such that $(\det(\alpha), N) = 1$. Then we obtain an isomorphism of $R(\Gamma_N, \Delta_N)$ onto $R(\Gamma, \Delta_N{}^*)$ by

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

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

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

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 $S_m(\Gamma_N)$: $\Gamma_N\alpha\Gamma_N \longrightarrow T_m(\Gamma_N\alpha\Gamma_N)$, we get a Dirichlet series with matrix coefficients

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

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

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 ∞ of Γ_1, each form f_j has a Fourier expansion

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

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

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

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

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

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

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 formulatio 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 Γ be a Fuchsian group of the first kind, and V a projective non-singular curve analytically isomorphic to H^*/Γ. Let Δ be as in the beginning of § 3. Denote by φ 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 Γ_N defined by (3.5) as our Γ. Let V_N be a projective non-singular model for H^*/Γ_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^*/Γ_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,

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

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

Here $(\ )_p$ means reduction modulo p, Π_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 ξ_p, η_p, ζ be the elements of $\mathrm{End}(J_N)$ corresponding to X_p, Y_p, Z. From our theorem it follows easily that

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

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

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

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

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_ℓ is equivalent to the direct sum of M^d and its complex conjugate. Since ξ_p and η_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 ξ_p (resp. η_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 $M_\ell(\pi_p)$ 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 ω_1, ω_2, x with the condition $\mathrm{Im}(\omega_1/\omega_2) > 0$, defined by

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

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

where $\sum{}'$ means the sum extended over all the elements ω, 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 γ by $j(z) = \gamma/(\gamma - 27)$ and call

$E(z)$ the elliptic curve $y^2 = 4x^3 - \gamma x - \gamma$. 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 $Q(j, f^N_{ab})$. 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^*/Γ_N and actually defined over Q.

Now let us consider a disjoint expression

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

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 $1 \leqq i \leqq p+1$. Since $\det(\alpha_i) = p$, one can find an isogeny λ_i of E_i to E_1 whose kernel is of order p. Then the $\operatorname{Ker}(\lambda_i)$ for $1 \leqq i \leqq p+1$ are exactly all the subgroups of order p of E_0. In view of (4.1), the modular correspondence X^N_p can be described by the mapping

$$(j(z_0), f^N_{ab}(z_0)) \longrightarrow \{(j(z_i), f^N_{ab}(z_i)) \mid 1 \leqq i \leqq p+1\},$$

or

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

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

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

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

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

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

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

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

By (5.2) and (5.4), reduction modulo P of (5.1) is

$$(5.5)\qquad (j_0, h_0(t))_P \longrightarrow (j_0^{\,p}, h_0(t)^p)_P + p \text{ times } (j_0^{\,1/p}, h_0(pt)^{1/p})_P \qquad (t \in E_0,\ Nt = 0).$$

It can be shown that the operation $(j_0, h_0(t)) \longrightarrow (j_0, h_0(pt))$ gives exactly Y_p^N on V_N. Therefore from (5.5) we obtain

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

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

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

The result was generalized by [10], whose method I followed in the above. The result for $\Gamma_0(N)$ or any congruence subgroup of Γ_1 is derivable essentially from the result for Γ_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 Φ be an indefinite quaternion algebra over Q, i.e., an algebra such that $\Phi \otimes_Q R$ is isomorphic to the total matrix algebra $M_2(R)$. Let $\mathfrak{o}$ be a maximal order in Φ, i.e., a maximal one among the subrings of Φ which are finitely generat modules over Z. We consider Φ 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 $\Phi = M_2(Q)$, these are nothing but Γ_1 and Γ_N considered in § 3. If Φ is a division algebra, they have compact quotient spaces.

Suppose that N is prime to the discriminant of Φ. 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 α 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 $R(\Gamma_N(\mathfrak{o}), \Delta_N(\mathfrak{o}))$ in $S_m(\Gamma_N(\mathfrak{o}))$, we can construct a Dirichlet series $D_m^N(s; \Phi)$ 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 Φ; and $\zeta^{(\Gamma)}(s; V_N(\mathfrak{o})/Q)$ 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) $$A_z = C^2/L_z, \quad L_z = \{ a \binom{z}{1} \mid a \in \mathfrak{o} \},$$

where an element of $\mathfrak{o}$ 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 $\mathfrak{o}$ 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 $\Gamma(\mathfrak{o})$ at z. The automorphic functions with respect to the congruence subgroup $\Gamma_N(\mathfrak{o})$ 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 $H/\Gamma_N(\mathfrak{o})$) with the isogenies of A_z. Using the same idea as in § 5, we obtain congruence relations for modular correspondences on $H/\Gamma_N(\mathfrak{o})$, 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

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

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

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

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 $7 \leqq \ell \leqq 97$.

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_ℓ 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_ℓ/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^*/Γ_N (or $H/\Gamma_N(\varepsilon)$), 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 χ of Q, we define a Dirichlet series

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

for $D_m^N(s;\phi) = \sum_{n=1}^{\infty} B_n n^{-s}$. Then $D_m^N(s;\chi;\phi)$ can be continued holomorphically on the whole s-plane and satisfies a functional equation [13, Th. 1 It is easy to see that $\zeta^{(1)}(s;V_N(\sigma)/k)$ is a product of $\det[D_2^N(s;\chi;\phi)]^{-1}$ for several χ'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 χ 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 χ. 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 ± 1 are only automorphisms of E, every isomorphism λ 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 $m \geqq 2$.

To construct such a fibre variety, take Φ and $\mathfrak{O}$ as in § 6; assume that Φ 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

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

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

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

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 $V_N = \Gamma_N(\sigma)\backslash H$, 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 Φ. 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 α_p and β_p of Δ, 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

$$\left.\begin{aligned}(X_p^{(h)})_p &= \prod_p + \prod_p^*,\\ p(Y_p^{(h)}) &= \prod_p \circ \prod_p^*,\end{aligned}\right. \qquad \text{on } (W_N^{(h)} \times W_N^{(h)})_p$$

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

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

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 collabotration with Kuga.

A formula of this kind was first given empirically by Sato for a certain fibre variety whose base is H^*/Γ_N and fibres are the product of elliptic curves modulo ± 1. A variety of this kind had been suggested by Kuga, as the one whihh 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 ζ 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, Sec. I, vol. VIII, Part 2, 363 - 386.

16. ________, On the ζ-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 ℓ-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 $\mathbb{Z}$.

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:

$$(1) \qquad \dim. X = \text{Kronecker dim. of } k(x).$$

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

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

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

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 $\mathbb{Z}$ or $\mathbb{F}_p$. 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* $\operatorname{char}. E = 0$, *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* $\operatorname{char}. E = p \neq 0$, *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* $\zeta(X, s)$

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

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. <u>Some properties and examples.</u>

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

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

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

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

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:

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

(This -- with $Y = \operatorname{Spec}(\underline{\underline{Z}})$ -- 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 $X = \operatorname{Spec}(A)$, where A is the ring of integers of a number field K, $\zeta(X, s)$ coincides with the classical zeta function ζ_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) $$\zeta(X, s) = Z(X, q^{-s}),$$

where $Z(X,t)$ is the power series defined by the product:

(6) $$Z(X,t) = \prod_{x \in \overline{X}} \frac{1}{1 - t^{\deg(x)}}$$

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:

$$(7) \qquad \log. Z(X,t) = \sum_{n=1}^{\infty} \nu_n t^n/n.$$

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 $\underline{O}_X$ 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 ν_n is *the number* $\Lambda(F^n)$ *of fixed points of* F^n. This remark, first made by Weil, is the starting point of his interpretation of ν_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 $\overline{Y}$ of Y may be identified with $\overline{X}/G$. More precisely, let $x \in \overline{X}$, let y be its image in $\overline{Y}$, 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 <u>étale</u> 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 <u>Frobenius element</u> of x.

2.2. <u>Artin's definition of L functions.</u>

Let χ be a character of G (i.e. a linear combination, with coefficients in $\underline{\underline{Z}}$, of irreducible complex characters). For each $y \in \overline{Y}$, and for each integer n, let $\chi(y^n)$ be the mean value of χ 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]):

$$\log. L(X,\chi;s) = \sum_{y\in\overline{Y}} \sum_{n=1}^{\infty} \chi(y^n)\, N(y)^{-ns}/n. \tag{8}$$

When χ is the character of a linear representation $g \mapsto M(g)$, one has:

$$L(X,\chi;s) = \prod_{y\in\overline{Y}} \frac{1}{\det(1 - M(F_x)/N(y)^s)}, \tag{9}$$

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. <u>Formal properties of the L functions.</u>

(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 χ'

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 π. Let χ' 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 χ'). 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 χ an irreducible character of G. One has:

$$(12) \qquad L(X, \chi ; s) = \frac{1}{1 - \chi(F)\, q^{-s}} ,$$

where F is the Frobenius element of G.

It is not hard to see that <u>properties</u> (i) <u>to</u> (vi) <u>characterize uniquely the L functions.</u>

(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 <u>irreducible characters</u> 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 $\mathbb{F}_q$ - scheme, and assume that the operations of G are $\mathbb{F}_q$ - automorphisms of X. The scheme $Y = X/G$ is then also an $\mathbb{F}_q$ - 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:

$$\text{(14)} \qquad \log . \underline{L}(X, \chi; t) = \sum_{n=1}^{\infty} \nu_n(\chi) t^n/n,$$

with:

$$\text{(15)} \qquad \nu_n(\chi) = \frac{1}{(G)} \sum_{g \in G} \chi(g^{-1}) \Lambda(gF^n),$$

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 $\mathbb{F}_q$: this follows from ℓ-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 $G = \mathbb{Z}/p\mathbb{Z}$ 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 $\mathbb{F}_q$ - scheme, and let a be a section of the sheaf $\underline{O}_Y$. In the affine line $Y[T]$, let X be the closed subscheme defined by the equation

$$T^p - T = a.$$

If we put $G = \mathbb{Z}/p\mathbb{Z}$, 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 $\mathbb{C}$, and let χ be the character of G defined by $\chi(n) = w^n$. The L function $\underline{L}(X, \chi; t)$ is given by formula (14); its coefficients $\nu_n(\chi)$ can be written here in the following form:

$$\nu_n(\chi) = \sum_{y \in Y_n} w^{\mathrm{Tr}_n a(y)}, \tag{16}$$

where $Y_n = Y(k_n)$, and Tr_n is the trace map from $k_n = \mathbb{F}_{q^n}$ to $\mathbb{F}_p$. The above expression is a typical "exponential sum". If, for instance, we take for Y the multiplicative group $\mathbb{G}_m$, 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

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

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* χ *be a character of* G, *and let* $\langle \chi, 1 \rangle$ *be the multiplicity of the identity character* 1 *in* χ. *The order of* $L(X, \chi)$ *at* $s = \dim. X$ *is equal to* $-\langle \chi, 1 \rangle$.

COROLLARY. *If* χ *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:

$$(19) \qquad \Big(\sum_{y \in M} \frac{1}{N(y)^s} \Big) / \log \frac{1}{s - n} \to m \qquad \text{for } s \to n.$$

(For $Y = \operatorname{Spec}(\underline{\underline{Z}})$, 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 $\dim. X \geqq 1$, 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_ $\operatorname{Card}(R)/\operatorname{Card}(G)$.

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.

TABLE OF CONTENTS

SEMINAR ON SINGULARITIES I

The seminar met five times. The speakers were Hironaka (July 14 and July 16), Zariski (July 21 and July 23) and Abhyankar (July 29.)

by

H. Hironaka

§1. A theorem of Whitney

Let $f = V^n \hookrightarrow \mathbb{C}^N$ be an imbedding of a complex-analytic variety V of dimension n ; a variety will be always assumed to be reduced and irreducible. Suppose V , identified with its image by f , goes through the origin O . If x is a simple point of V , then $T_x(f)$ will denote the tangent space of V at x , which is canonically identified with a linear subspace of $\mathbb{C}^N$, the last being viewed as the tangent space of $\mathbb{C}^N$ at each point. We have an ordinary inner product in the vector space $\mathbb{C}^N$, denoted by $u \cdot v = \sum_{i=1}^N u_i \cdot \overline{v_i}$ if $u = (u_1, \ldots, u_N)$ and $v = (v_1, \ldots, v_N)$. We define the normal vector space, $N_x(f)$, of V at x as the orthogonal complement of the tangent space $T_x(f)$ in $\mathbb{C}^N$. Let $V_0 = V - S(V) \cup \{O\}$, where $S(V) =$ the singular locus of V . Let us consider

$$\rho(f;x) = \max_{\begin{pmatrix} v \in N_x(f) \\ v \neq 0 \end{pmatrix}} \left\{ \frac{|v \cdot \overrightarrow{Ox}|}{|v| \cdot |\overrightarrow{Ox}|} \right\}$$

where $x \in V_0$ and $\overrightarrow{Ox}$ = the vector joining the origin to x in the vector space $\mathbb{C}^N$ Let us also consider

$$\tau(f;x) = \max_{\begin{pmatrix} v \in T_x(f) \\ v \neq 0 \end{pmatrix}} \left\{ \frac{|v \cdot \overrightarrow{Ox}|}{|v| \cdot |\overrightarrow{Ox}|} \right\}$$

for $x \in V_0$. We have the equality

$$\tau(f ; x)^2 + \rho(f ; x)^2 = 1 .$$

Theorem (1.1) (Whitney)

$$\lim_{x \longrightarrow 0} \rho(f ; x) = 0$$

or, equivalently,

$$\lim_{x \longrightarrow 0} \tau(f ; x) = 1$$

where x runs through the non-singular part of V, other than the origin.

Proof. First consider the case of $\dim V = 1$. Clearly, we may assume that V is irreducible. Let t be a uniformizing parameter on the normalization of V at the point above O. Then the coordinate functions $x_i = x_i(t)$ $(1 \leq i \leq N)$ are holomorphic functions in t. Now, obviously

$$\tau(f\,;\,x(t)) = \frac{\left|\sum_{i=1}^{n} x_i(t)\,\overline{x_i'(t)}\right|}{\sqrt{\sum_{i=1}^{n}|x_i'(t)|^2}\sqrt{\sum_{i=1}^{n}|x_i(t)|^2}}.$$

Let p be the minimum of the orders of $x_i(t)$, which is positive because V goes through O. Let $\operatorname{ord}(x_1(t)) = p$, for instance. Then $\lim_{t\to 0}\frac{x_i(t)}{x_1(t)} = \lim_{t\to 0}\frac{x_i'(t)}{x_1'(t)}$ for all i so that $\lim_{t\to 0}\tau(f\,;\,x(t)) = 1$.

Next consider the general case. The proof will be reduced to the above case. Let us choos a birational blowing-up $\pi_0 : \tilde{V}_0 \longrightarrow V$ such that, V_0 being the non-singular part of V outside the origin O, π induces an isomorphism of $\pi^{-1}(V_0)$ to V_0 and the holomorphic map of V_0 to the Grassmannian $G_{N,n}$, $x \in V_0 \longrightarrow T_x(f)$, extends holomorphically through $\tilde{V}_0$. (For instance, let $\tilde{V}_0$ be the graph of the meromorphic map defined by the above $V_0 \longrightarrow G_{N,n}$.) Then let $\pi : \tilde{V} \longrightarrow V$ be the composition of π_0 and the birational blowing-up of the ideal on $\tilde{V}_0$ generated by the x_i. Again, $\pi : \pi^{-1}(V_0) \xrightarrow{\approx} V_0$, and $V_0 \longrightarrow G_{N,n}$ extends through $\tilde{V}$. Now, at each point $\tilde{x} \in \tilde{V}$, we can find d independent holomorphic vectors which span $T_x(f)$ for all $x \in V_0 = \pi^{-1}(V_0)$ in a certain neighborhood of $\tilde{x}$ in $\tilde{V}$, and moreover there exists an index q such that the ratios x_j/x_q are all holomorphic at $\tilde{x}$ for $1 \leq j \leq N$. It is now easy to show that the function $\tau(f\,;\,x)$ for $x \in V_0$ extends continuously through $\tilde{V}$. Now, to prove the theorem, suppose it were false. Then there exists a point $\tilde{x} \in \tilde{V}$ such that $\pi(\tilde{x}) = 0$ and the extended $\tau(f\,;\,x)$ takes a value $\neq 1$ at $\tilde{x}$. Take then an irreducible curve through $\tilde{x}$, say $\tilde{\Gamma}$, which is not contained in $\tilde{V} - V_0$. We may assume that $\tilde{\Gamma} - \{\tilde{x}\} \subset V_0$. Let $\Gamma = \pi(\tilde{\Gamma})$, and $g : \Gamma \hookrightarrow \mathbb{C}^N$ be the imbedding induced by f. Then, clearly by the definition, $\tau(g\,;\,x) \leq \tau(f\,;\,x)$ for all $x \in \Gamma - \{0\}$. Then $\lim_{x\to 0}\tau(g\,;\,x) \leq \lim_{x\to 0}\tau(f\,;\,x) < 1$, which contradicts the above result in the 1-dimensional case. Q.E.D.

We are here particularly interested in the case of isolated singular point, say $0 \in V \hookrightarrow \mathbb{C}^N$. Then the above theorem shows that the function $\rho(f\,;\,x)$ for

$x \in V - \{0\}$, where $f : V \longrightarrow \mathbb{C}^N$, extends to a continuous function on V so that $\rho(f ; 0) = 0$; the same for $\tau(f ; x)$ with $\tau(f ; 0) = 1$. From now on, we shall use the symbols $\rho(f ; x)$ and $\tau(f ; x)$ in this extended sense.

Remark (1.2) Let $(F_1, \ldots, F_r)$ be a base of the ideal of V^n in $\mathbb{C}^N$ at the origin. Let J_0 be the ideal on V generated by the $(N-n)\times(N-n)$-minors of the Jacobian $\partial(F_1, \ldots, F_r)/\partial(X_1, \ldots, X_N)$. Then the closure V_0 of the graph of $V_0 \longrightarrow G_{N,n}$ in $V \times G_{N,n}$ (cf. The above proof of Theorem (1.1)) is the birational blowing-up of $\mathcal{J}$, with reference to the morphism $\pi : \tilde{V}_0 \longrightarrow V$ induced by the projection from $V \times G_{N,n}$

Remark (1.3) Let S_ε be a sphere of real dimension $2N-1$ in $\mathbb{C}^N$ with radius $\varepsilon > 0$ and with center O. Let x be a point of $S_\varepsilon \cap V$. Then the tangent space $T_x(S_\varepsilon)$ is naturally identified with a $\mathbb{R}$-subspace of $\mathbb{C}^N$, and it contains an $N-1$ dimensional $\mathbb{C}$-subspace of $\mathbb{C}^N$. Denote this by $T_x^o(S_\varepsilon)$. Then one can see that $T_x^o(S_\varepsilon)$ is orthogonal to the vector $\overrightarrow{Ox}$, and $S_\varepsilon \cap V$ is transversal at x if and only if $T_x^o(S_\varepsilon)$ does not contain $T_x(V)$ ($= T_x^o(V)$). Thus we get: $S_\varepsilon \cap V$ is transversal at $x \Leftrightarrow \tau(f; x) > 0 \Longleftrightarrow \rho(f; x) < 1$. Therefore, by Th. (1.1), there exists a positive number ρ such that $S_\varepsilon \cap V$ is transversal for all ε with $0 < \varepsilon < \rho$.

§2. Continuity of W-function.

Let (π, X, Y, ε) be a family of isolated singular points of complex-analytic varieties. (cf. My note on "Equivalences and Deformations of Isolated Singular Points".) This means that X, Y are reduced complex-analytic spaces; π and ε are holomorphic maps such that $\pi \circ \varepsilon$ = identity ; π is flat; all the fibres X_y, $y \in Y$, are reduced and equidimensional; finally, X is locally isomorphic to a domain in $Y \times \mathbb{C}^n$ at every point of $X - \varepsilon(Y)$, where $n = \dim X_y$. Suppose we have a permissible imbedding $f : X \hookrightarrow Y \times \mathbb{C}^N$. Namely, f is an imbedding such that π = (projection)$\circ f$ and $\varepsilon(Y) = Y \times 0$. Then we define $\tau(f ; x)$ and $\rho(f ; x)$ on X. (cf. The above cited note.) Assume: Y is non-singular irreducible.

I shall prove:

Theorem (2.1) The condition (ES) on the permissible imbedding $f : X \hookrightarrow Y \times \mathbb{C}$ implies the continuity of $\tau(f ; x)$.

Proof: Recall Definition 2 of the note cited above. We have an ideal sheaf $\mathcal{J}$ on X, which is the product $\mathcal{I}\mathcal{J}_0$, where $\mathcal{I}$ is the ideal sheaf of $\varepsilon(Y)$ on X and $\mathcal{J}_0$ is the ideal sheaf generated by the $(N-n)\times(N-n)$-minors of the Jacobian of the defining equations of X in $Y \times \mathbb{C}^N$ with respect to the coordinate functions on $\mathbb{C}^N$. Let $\tilde{h}: \tilde{X} \to X$ be the birational blowing-up of $\mathcal{J}$ followed by the normalization. Let $\tilde{\mathcal{J}}$ be the ideal sheaf on $\tilde{X}$ generated by $\mathcal{J}$, and $\tilde{Y}$ the complex subspace of $\tilde{X}$ defined by $\mathcal{J}$. The flatness of $\tilde{Y} \longrightarrow Y$ (which is the condition (ES)) implies that every irreducible component of $\tilde{Y}$ is mapped onto Y. This implies that for every point y of Y, $\tilde{h}^{-1}(X_y)$ is equal to the closure of $\tilde{h}^{-1}(X_y - \mathcal{E}(y))$ in $\tilde{X}$. Now I claim: $\tau(f\,;\,x)$ on $X - \mathcal{E}(Y) \cong \tilde{h}^{-1}(X - \mathcal{E}(Y))$ extends continuously through $\tilde{X}$, and the extension is zero at every point of $\tilde{X} - \tilde{h}^{-1}(X - \mathcal{E}(Y)) = \tilde{h}^{-1}(\mathcal{E}(Y))$. Note the second assertion follows the first, by what we have proven above and by Whitney's theorem. The first assertion, on the other hand, is a consequence of the facts that: (i) $\mathcal{J}\underline{O}_{\tilde{X}}$ is invertible as $\underline{O}_{\tilde{X}}$- modules; and (ii) $\mathcal{J}_0\underline{O}_{\tilde{X}}$ is invertible, so that the natural map $X - \mathcal{E}(Y) \longrightarrow Y \times G_{N,n}$ (cf. Remark (1, 2)) is holomorphically extended to $\tilde{X} \longrightarrow Y \times G_{N,n}$, where $X - \mathcal{E}(Y)$ is identified with $\tilde{X} - \tilde{h}^{-1}(\mathcal{E}(Y))$. Q.E.D.

SEMINAR ON SINGULARITIES, II

by

O. Zariski

§ 3. Let x, y, t be complex variables and let $f(x, y, t) = y^n + a_1(x, t)y^{n-1} + \dots + a_n(x, t)$, where the $a_i(x, t)$ are holomorphic function at $x = t = 0$ (and f has no multiple factors.) Assume that $f(0,0,t) = 0$ and that the y-discriminant of f is of the form $\mathcal{E}(x,t)\, x^q$, $q \geqq 0$, $\mathcal{E}(0,0) \neq 0$ (this means that the surface $f = 0$ is equisingular at the origin, along the line $x = y = 0$; see Zariski's lecture "Equisingularity etc.").

Fix $\delta > 0$ such that the power series $a_i(x,t)$ are convergent and that $\mathcal{E}(x,t) \neq 0$ for all (x,t) such that $|x| < \delta$, $|t| < \delta$.

Notations:

$\mathbb{A}$: the affine 3-space of the variables x, y, t.

V : the set of points (x,y,t) of the surface $f = 0$ such that $|x| < \delta$, $|t| < \delta$.

E_0 : $\{(x,y) \mid |x| < \delta, \text{ y-arbitrary}\}$.

T : the disc $|t| < \delta$.

V_0 : the section of V with the plane $t = 0$.

The full details of Whitney's proof of the following theorem were given:

<u>Theorem. There exists a homeomorphism</u> Ψ <u>of</u> $E_0 \times T$ <u>into</u> $\mathbb{A}$ <u>such that:</u>

1) $\Psi(V_0 \times T) = V$.

2) <u>For any</u> $(x,y) \in E_0$ <u>and</u> $t \in T$, <u>we have</u> $\Psi((x,y) \times t) = (x, \phi(x,y,t), t)$, <u>where</u> ϕ <u>is some continuous function on</u> $E_0 \times T$.

3) <u>The function</u> ϕ <u>has the following properties:</u>

3a) $\phi(x,y,0) = y$.

3b) ϕ <u>is analytic in</u> t.

3c) ϕ <u>is real analytic in</u> x,y,t, <u>except perhaps</u> 1) <u>at the points where</u> $x = 0$ and 2) <u>at the points of</u> $V_0 \times 0$.

<u>The construction of the function</u> $\phi(x,y,t)$.

A) One first constructs (and this is the easy part) a function ϕ_1 on $V_0 \times T$ which will play the role of the restriction of ϕ to $V_0 \times T$. Let $y_i(x,t)$ be the n distinct solutions of $f(x,y,t) = 0$ ($0 \neq |x| < \delta$, $|t| < \delta$) and let

(1) $\eta_i(x) = y_i(x,0)$.

For any point $(x, \eta, 0)$ of V_0 $(f(x, \eta, 0) = 0,\ x \neq 0)$, one and only one of the n (holomorphic) functions $y_i(x,t)$ has the property that $y_i(x', t) \longrightarrow \eta$ as $(x', t) \longrightarrow (x, 0)$. If $y_i(x,t)$ is that function, we set

$$(2) \qquad \begin{aligned} \phi_1(x, \eta, t) &= y_i(x, t), \quad \text{if } x \neq 0 \\ \phi_1(0,0,t) &= 0 . \end{aligned}$$

B) We now extend ϕ_1 to a function ϕ on $E_0 \times T$. If $y_1, y_2, \ldots, y_n$ are complex numbers and $y \neq y_i$, all i, set

$$\mu_i = \frac{1}{|y - y_i|}, \quad \nu_i(y_1, y_2, \ldots, y_n, y) = \frac{\mu_i}{\sum_{j=1}^{n} \mu_j} .$$

The ν_i are real-valued, non-negative, real analytic functions, defined outside the n planes $y = y_i$. If for a given i we have $y_i \neq y_j$ for all $j \neq i$ then the ν_i is also defined and continuous at $(y_1, y_2, \ldots, y_n, y_j)$ (all j) and $\nu_i(y_1, y_2, \ldots, y_n, y_j) = \delta_{ij}$.

For $0 \neq |x| < \delta$ set

$$\sigma_i(x,y) = \nu_i(\eta_1(x), \eta_2(x), \ldots, \eta_n(x), y),$$

where the $\eta_i(x)$ are defined in (1). Then define the function $\phi(x,y,t)$ as follows:

$$(3) \quad \begin{cases} \phi(x,y,t) = y + \sum_{i=1}^{n} \sigma_i(x,y) \left[y_i(x,t) - \eta_i(x) \right], \\ \qquad\qquad\qquad\qquad \text{if } (x, y) \neq (0, 0) . \\ \phi(0,0,t) = 0 . \end{cases}$$

Then ϕ is defined and continuous on $E_0 \times T$ and has the properties 3a), 3b) and 3c) stated in the theorem. The proof that the mapping Ψ of $E_0 \times T$ into A defined by $\Psi((x,y) \times t) = (x, \phi(x,y,t), t)$ is a homeomorphism depends on showing that if δ is sufficiently small then

(4) $\phi(x, y', t) \neq \phi(x,y,t)$ for all x, y, y', t such that $|x| < \delta$, $|t| < \delta$ and $y \neq y'$.

The proof of (4) is based on two facts.

B1) By elementary calculus one shows that if $b_1, b_2, \ldots, b_n$ are complex numbers and if

$$\gamma = \max\left\{\frac{|b_i - b_j|}{|y_i - y_j|}\right\} \qquad (y_i \neq y_j \quad \text{if} \quad i \neq j)$$

then

$$(5) \left|\sum_i (\nu_i(y_1, y_2, \ldots, y_n, y') - \nu_i(y_1, y_2, \ldots, y_n, y))\, b_i\right| \leqq 4\gamma(n-1)\,|y' - y|.$$

From (5) and (3) it follows that if the absolute values of the

$$(6) \qquad \frac{\Delta_i(x,t) - \Delta_j(x,t)}{\eta_i(x) - \eta_j(x)},$$

where $\Delta_i(x,\eta) = y_i(x,t) - \eta_i(x)$, are bounded in the region $0 \neq |x| < \delta$, $|t| < \delta$, say if

$$(7) \qquad \frac{|\Delta_i(x,t) - \Delta_j(x,t)|}{|\eta_i(x) - \eta_j(x)|} \leqq \gamma \qquad (\text{all } i,j,\ i \neq j),$$

then

$$(8) \qquad \left|\frac{\phi(x,y',t) - \phi(x,y,t)}{y' - y} - 1\right| \leqq 4\gamma(n-1),$$

for all x, y, y', t such that $|x| < \delta$, $|t| < \delta$, $y \neq y'$.

B2) To say that the (7) are valid for some γ is the same as saying that the quotients (6) are <u>integral</u> functions of x and t. This is in fact the case and is a consequence of our assumption that the discriminant of f is of the indicated form $\varepsilon(x,t)\, x^q$, $\varepsilon(0,0) \neq 0$. Then it follows that these quotients have value zero at $x = t = 0$. Therefore if δ is sufficiently small then, in (7), we can assume $\gamma < \frac{1}{4(n-1)}$, and then (4) follows from (8).

§4. We consider now, more generally, an algebroid hypersurface

$$(1) \qquad f(x_1, x_2, \ldots, x_s, y, t) = 0$$

in the complex affine $(s+2)$-space $\mathbb{A}$ of the variables $x_1, x_2, \ldots, x_s, y, t$. We assume that f is a monic polynomial in y, of degree n, with coefficients which are power series in $x_1, x_2, \ldots, x_s, t$, convergent in the region $|x_i| < \delta$ $(i = 1, 2, \ldots,$ $|t| < \delta$. If $D(x_1, x_2, \ldots, x_s, t)$ is the y-discriminant of f and π denotes the projection $(x_1, x_2, \ldots, x_s, y, t) \longrightarrow (x_1, x_2, \ldots, x_s, t)$ of the hypersurface (1) onto the affine $(s+1)$-space $\mathbb{A}'$ of the variables $x_1, x_2, \ldots, x_s, t$, then the hypersurface

$$\Delta \ : \ D = 0$$

in $\mathbb{A}'$ is the critical variety of the mapping π.

In the case $s = 1$ we have assumed (§3) that Δ is the line $x_1 = 0$. In that case, a neighborhood of Δ in $\mathbb{A}'$ is a topological (and even analytical) direct product $E_0' \times T$, where E_0' is the line $t = 0$ and T is the disc $|t| < \delta$, with Δ being the fibre $0 \times T$. We shall now make a similar assumption on Δ in the general case, as follows:

<u>Notations:</u>

Δ : the set of points $(x_1, x_2, \ldots, x_s, t)$ of the critical variety $D = 0$ such that $|x_i| < \delta$ $(i = 1, 2, \ldots, s)$, $|t| < \delta$.

$$E_0' = \{(x_1, x_2, \ldots, x_s) \mid |x_i| < \delta\}.$$

T : the disc $|t| < \delta$.

Δ_0' : the section of Δ with the space $t = 0$.

We make the following "<u>direct product</u>" <u>assumption</u>:

There exists a homeomorphism Ψ' of $E_0' \times T$ into $\mathbb{A}'$ such that:

1) $\Psi'(\Delta_0' \times T) = \Delta$.
2) $\Psi'((x_1, x_2, \ldots, x_s) \times t) = (x_1', x_2', \ldots, x_s', t)$, where the x_i' are some functions of $x_1, x_2, \ldots, x_s, t$.
3) $\Psi'((x_1, x_2, \ldots, x_s) \times 0) = (x_1, x_2, \ldots, x_s, 0)$.
4) The fibres $F_x = \Psi'((x) \times T)$ are analytic (isomorphic to T).
5) If $P_0 = (x) \times 0 \in \Delta$ and if $\Delta_1, \Delta_2, \ldots, \Delta_h$ are the analytically irreducible components of Δ at P_0, then F_x lies on each of Δ_j.

If $\bar{P} = (\bar{x}) \times \bar{t}$ is any point of $E_0 \times T$, let m denote the number of distinct roots of $f(\bar{x}_1, \ldots, \bar{x}_s, y, \bar{t})$, and let $n_1, n_2, \ldots, n_m$ be the multiplicities of these roots $(n = \sum n_j)$. The integers m, n_j are functions of $\overline{P}$. From the "direct product" assumption follows that locally at $\overline{P}$, the fundamental group of $\mathbb{A}' - \triangle$ is the same as the fundamental group of $\mathbb{A}'' - \triangle_{\overline{t}}$, where $\mathbb{A}''$ is the hyperplane $t = \overline{t}$ and $\triangle_{\overline{t}}$ is the section of $\triangle$ with that hyperplane. Using this and an appropriate Galois theory argument, it is possible to prove the following:

__Lemma.__ __The functions__ $m(P)$, $n_1(P), \ldots, n_{m(P)}(P)$ __are constant along each fibre__ F_x (provided δ is sufficiently small).

This lemma shows that the inverse image $\pi^{-1}(F_x)$ of each fibre F_x is the union of $m(P)$ $(P \in F_x)$ non-intersecting analytic fibres, isomorphic to F_x . Thus the fibration $\{F_x\}$ can be lifted to the hypersurface $V: f = 0$, and this yields a homeomorphism Ψ_1 of $V_0 \times T$ onto V (V_0 = section of V with $t = 0$) such that if $(x_1, x_2, \ldots, x_s, \eta, 0) \in V_0$ then $\Psi_1((x, \eta) \times t) = (x_1', x_2', \ldots, x_s', \phi_1(x_1, x_2, \ldots, x_s, \eta, t), t)$, where $(x_1', x_2', \ldots x_s', t) = \Psi'((x) \times t)$ and $\phi_1(x, \eta, t) = y_i(x', t)$, $y_i(x,t)$ being that root of $f(x,y,t) = 0$ which approaches η as $t \longrightarrow 0$.

If we now wish to use Whitney's method for the purpose of extending Ψ_1 to a homeomorphism of $E_0 \times T$ into $\mathbb{A}$ (where $E_0 = \{(x_1, x_2, \ldots, x_s, y)\} \mid |x_i| < \delta$, $i = 1, 2, \ldots, s$; δ sufficiently small), then it is necessary to assume that all the quotients

$$\frac{y_i(x,t) - y_j(x,t)}{y_i(x,0) - y_j(x,0)} \qquad , \qquad i \neq j,$$

are integral functions of $x_1, x_2, \ldots, x_s$, t. This is easily seen to be equivalent to assuming that the y-discriminant D of f is of the form $\varepsilon(x_1, x_2, \ldots, x_s, t) D_0(x_1, x_2, \ldots, x_s)$ with $\varepsilon(0, 0, \ldots, 0) \neq 0$.

This is precisely the assumption of "analytical equisingularity" of the critical variety made in §4 of Zariski's lecture "Equisingularity etc.". This proves the final statement made at the very end of that lecture.

The algebraic (or algebroid) structure of V in this particular case requires further study.

NONSPLITTING

by

S. Abhyankar
Purdue University

<u>Definition 1.</u> Let R be a positive dimensional regular local domain with quotient field K. Let M be the maximal ideal in R. We get a real discrete valuation of K by taking the value of x/y to be $a - b$ where x and y are any nonzero elements in R and a and b are the greatest integers such that $x \in M^a$ and $y \in M^b$. This valuation is denoted by ord_R.

<u>Notation.</u> Henceforth R will denote a two dimensional regular local domain with quotient field K such that R is of characteristic $p \neq 0$ and the residue field of R is algebraically closed.

In the second paragraph on page 13 of my talk "Current status of the resolution problem" I stated a result concerning "local nonsplitting". The main part of the proof of that result is the proof of the following theorem which is a special case of that result.

<u>THEOREM. Let</u> L <u>be a Galois extension of</u> K <u>of degree</u> p <u>and let</u> v <u>be a real nondiscrete valuation of</u> K <u>dominating</u> R <u>such that</u> v <u>has only one extension to</u> L. <u>Let</u> R_n <u>be the</u> n^{th} <u>quadratic transform of</u> R <u>along</u> v. <u>Then there exists a positive integer</u> m <u>such that for all</u> $n \geqq m$ <u>we have that</u> ord_{R_n} <u>has only one extension to</u> L.

In turn, the proof of the above theorem follows from the following three lemmas.

<u>Definition 2.</u> Given a monic polynomial $f(Z)$ in an indeterminate Z with coefficients in K and given a basis (x, y) of the maximal ideal in R, we shall say that $f(Z)$ is of $[R, x, y]$-<u>type</u> (u, v, a, b, c) provided

$$f(Z) = Z^p - (Dx^u y^v)^{p-1} Z + x^a y^b F$$

where: $u, v, a, b,$ are nonnegative integers; D is a unit in R; F is a nonzero element in R; $c = \mathrm{ord}_{R/xR}\, h(F)$ where $h\colon R \longrightarrow R/xR$ is the natural epimorphism; $u > 0$, $a < p$, $b < p$, $c \leqq 1$; if $a = 0$ then $b + c \not\equiv 0 (p)$; if $c = 1$ then $b = 0$; if $b \neq 0$ then $v \neq 0$.

<u>Definition 3.</u> Given a monic polynomial $f(Z)$ in Z with coefficients in K we shall say that $f(Z)$ is R-<u>typical</u> if there exists a basis (x, y) of the maximal ideal in R and there exist nonnegative integers $u, v, a, b, c,$ such that $f(Z)$ is of $[R, x, y]$-type (u, v, a, b, c).

<u>Definition 4.</u> Given a Galois extension L of K we shall say that L is <u>nice</u> relative to R if there exists a primitive element z of L over K such that the minimal monic polynomial of z over K is R-typical.

<u>Definition 5.</u> Given monic polynomials $f(Z)$ and $g(Z)$ of degree p in Z with coefficients in R we shall say that $g(Z)$ is an R-<u>translate</u> of $f(Z)$ if there exist elements r and s in R such that $r \neq 0$ and $g(Z) = r^{-p} f(rZ + s)$.

LEMMA 1. <u>Let</u> L <u>be a Galois extension of</u> K <u>of degree</u> p <u>and let</u> v <u>be a real nondiscrete valuation of</u> K <u>dominating</u> R <u>such that</u> v <u>has only one extension to</u> L. <u>Let</u> R_n <u>be the</u> n^{th} <u>quadratic transform of</u> R <u>along</u> v. <u>Then there exists a positive integer</u> m <u>such that</u> L <u>is nice relative to</u> R_m.

LEMMA 2. <u>Let</u> L <u>be a Galois extension of</u> K <u>such that</u> L <u>is nice relative to</u> R. <u>Then</u> ord_R <u>has only one extension to</u> L.

LEMMA 3. (Stability). <u>Let</u> $f(Z)$ <u>be a monic polynomial of degree</u> p <u>in</u> Z <u>with coefficients in</u> R <u>such that</u> $f(Z)$ <u>is</u> R-<u>typical</u>. <u>Then given any quadratic transform</u> S <u>of</u> R <u>there exists an</u> S-<u>translate</u> $g(Z)$ <u>of</u> $f(Z)$ <u>such that</u> $g(Z)$ <u>is</u> S-<u>typical</u>.

The proofs of Lemmas 2 and 3 are quite easy. The proof of Lemma 1 is algorithmic.

FURTHER COMMENTS ON BOUNDARY POINTS

by

David B. Mumford

In these notes, I shall describe some joint work of A. Mayer and myself as well as some related results, summarizing further comments made in my lecture and a 2nd lecture by Mayer. During the institute, lectures were also given by H. Rauch and L. Ehrenpreis discussing various aspects of the Torelli and Teichmüller covering spaces of the moduli scheme for curves of genus g (cf. the notes of Ehrenpreis). The ground field will be assumed to be the complex numbers in our discussion. One word of apology: the full proofs of many of our results have not been written down, so strictly speaking, much of what follows should be taken as conjectures not theorems.

§1. Compact moduli spaces for vector bundles over curves.

This theory has been worked out by Seshadri, Narasimhan, and myself. Let $\mathbb{E}$ be a vector bundle of rank r over a curve C.

Definitions:

i) $\mathbb{E}$ is regular if the only endomorphisms of $\mathbb{E}$ are multiples of the identity.

ii) $\mathbb{E}$ is stable if, for all sub-bundles $\mathbb{F} \subset \mathbb{E}$, $\deg\left[c_1(\mathbb{F})\right] < \frac{\text{rank }(\mathbb{F})}{\text{rank }(\mathbb{E})} \cdot \deg\left[c_1(\mathbb{E})\right]$,

iii) $\mathbb{E}$ is semi-stable if, for all sub-bundles $\mathbb{F} \subset \mathbb{E}$, $\deg\left[c_1(\mathbb{F})\right] \leq \frac{\text{rank }(\mathbb{F})}{\text{rank }(\mathbb{E})} \cdot \deg\left[c_1(\mathbb{E})\right]$,

iv) $\mathbb{E}$ is retractable if it is a direct sum of stable bundles.

If $\deg\left[c_1(\mathbb{E})\right] = 0$, $\mathbb{E}$ is retractable if and only if $\mathbb{E}$ admits a hermitian structure with curvature form 0.

To obtain a modulus space for vector bundles with given rank and $\deg(c_1)$, first one must throw out irregular bundles since they give rise to jump phenomenon, i.e., constant families of bundles, which suddenly jump to another bundle (cf. my lecture notes, "Curves on an algebraic surface", Lecture 7, §4). In the remaining class of bundles, the topology is still un-separated; but in the set of retractable bundles the topology is both compact and separated, since this set of bundles is isomorphic to the set of unitary representations of π_1 of the base curve (for $\deg\left[c_1(\mathbb{E})\right] = 0$; otherwise the argument can be modified). This set turns out to contain the open set of stable bundles, and to be contained in the open set of semi-stable bundles (it is not open itself). One finds that the stable bundles are classified by the points of a non-singular variety V, and that V is an open subset of a <u>compact</u> variety $\overline{V}$. The set of points of $\overline{V}$ is isomorphic to the (non-algebraic) set of retractable bundles, and there is even a natural map from the set of all semi-stable bundles to $\overline{V}$, but non-isomorphic bundles no longer correspond to distinct points:

$$\begin{tikzcd}
\left\{\begin{matrix}\text{regular}\\ \text{bundles}\end{matrix}\right\} \arrow[r, phantom, "\supset"] & \left\{\begin{matrix}\text{stable}\\ \text{bundles}\end{matrix}\right\} \arrow[r, phantom, "\cong"] \arrow[d, phantom, "\cap"] & \left\{\begin{matrix}\text{points of}\\ V\end{matrix}\right\} \arrow[d, phantom, "\cap"] \\
& \left\{\begin{matrix}\text{retractable}\\ \text{bundles}\end{matrix}\right\} \arrow[r, phantom, "\cong"] \arrow[d, phantom, "\cap"] & \left\{\begin{matrix}\text{points of}\\ \overline{V}\end{matrix}\right\} \\
& \left\{\begin{matrix}\text{semi-stable}\\ \text{bundles}\end{matrix}\right\} \arrow[ur] &
\end{tikzcd}$$

§2. <u>Compact moduli spaces for abelian varieties</u>: <u>Satake</u>

Let V_n denote the moduli scheme for principally polarized abelian varieties of dimension n. That is,

$$V_n \cong \mathfrak{H}_n / \Gamma_n \qquad \text{(as analytic space)}$$

where $\mathfrak{H}_n$ is the Siegel upper $\frac{1}{2}$-plane of type n, and Γ_n is the modular group acting on $\mathfrak{H}_n$. V_n has even a canonical structure of algebraic variety over $\mathbb{Q}$, due to its interpretation as a moduli scheme*. V_n carries a canonical class of ample invertible sheaves $\mathcal{L}(i)$ defined for all sufficiently large i, and such that

$$\mathcal{L}(i) \otimes \mathcal{L}(j) = \mathcal{L}(i + j)$$

when this makes sense. Therefore one has the graded ring

$$R_n = \bigoplus_{i \geq i_0} \Gamma(V_n, \mathcal{L}(i))$$

which is known to be isomorphic to the ring of modular forms on $\mathfrak{H}_n$ with respect to Γ_n, if $n \geq 2$.

---

*cf. Baily's work, or my "Geometric Invariant Theory".

The Satake compactification of V_n is then the open immersion:

$$V_n \subset \operatorname{Proj}(R_n) = V_n^*.$$

It turns out that there is a canonical isomorphism of $V_n^* - V_n$ and V_{n-1}^*, so that set-theoretically:

$$V_n^* = V_n \cup V_{n-1} \cup \text{------} \cup V_1 \cup V_0 \,.$$

(V_0 is a single point). This amazing equation suggests that this compact variety, which is defined only as a kind of "minimal model", should have an interpretation as a moduli space. In fact, consider all commutative group schemes X connected and of finite type over $\mathbb{C}$.

<u>Definition:</u> X is <u>stable</u> if X is an abelian variety.

X is <u>semi-stable</u> if X is an extension of an abelian variety by multiplicative groups $(\mathbb{G}_m)^r$.

X is <u>retractable</u> if X is the product of an abelian variety by multiplicative groups.

Exactly as before, A. Mayer and I have proven:

$$\begin{tikzcd}
\left\{\begin{array}{c}\text{Stable } X \text{ with}\\ \text{polarization}\end{array}\right\} \arrow[r, phantom, "\cong"] \arrow[d, phantom, "\cap"] & \left\{\begin{array}{c}\text{points of}\\ V_n\end{array}\right\} \arrow[d, phantom, "\cap"] \\
\left\{\begin{array}{c}\text{retractable } X\\ \text{with polarization}\end{array}\right\} \arrow[r, phantom, "\cong"] \arrow[d, phantom, "\cap"] & \left\{\begin{array}{c}\text{points of}\\ V_n^*\end{array}\right\} \\
\left\{\begin{array}{c}\text{semi-stable } X\\ \text{with polarization}\end{array}\right\} \arrow[ur] &
\end{tikzcd}$$

<u>Explanations</u>

1^o A polarization of X may be taken to mean a divisor D on X, determined up to algebraic equivalence, such that if

$$\pi : X \longrightarrow X_0$$

is the projection of X onto its abelian part, and if $D = \pi^*(D_0)$ (recall that $\mathrm{Pic}(X) \cong \mathrm{Pic}(X_0)$), then D_0 is ample on X_0 and

$$\begin{cases} \left(D_0^{n_0}\right) = n_0! \\ n_0 = \dim X_0 . \end{cases}$$

2^o A family of these objects is a morphism

$$f : \mathcal{X} \longrightarrow S$$

with the structure of group scheme (i.e., a "multiplication" μ: $\mathcal{X} \underset{S}{\times} \mathcal{X} \longrightarrow \mathcal{X}$, etc.) and a family of Cartier divisors $\mathcal{D}$ on $\mathcal{X}$ determined up to algebraic equivalence, and replacements

$$\mathcal{D}' = \mathcal{D} + f^*(\mathcal{E})$$

for any Cartier divisors $\mathcal{E}$ on S, and inducing a polarization of each fibre $f^{-1}(s)$. With this definition, stable and semi-stable $\mathcal{X}$'s form open sets, but retractable $\mathcal{X}$'s do not.

3^o The meaning of the arrows in the diagram is this: let $f : \mathcal{X} \longrightarrow S$ be a family of semi-stable objects where S is a <u>normal</u> algebraic variety. Map S to V_n^* by assigning to each $s \in S$ the point of V_{n_0} corresponding, in the classical way, to the abelian part of $f^{-1}(s)$. (n_0 = dim of this abelian part). Then this is a <u>morphism</u>.

This last result is proven by reducing to the case where S is a curve. Then one passes to the corresponding analytic set-up, and replaces S by a disc $\{z \mid |z| < 1\}$ where all fibres of f are diffeomorphic except for $f^{-1}(0)$. Next one introduces the invariant and vanishing cycles on the general fibre, so as to put the period matrix $\Omega_{ij}(z)$ of the abelian part of $f^{-1}(z)$ in a normalized form. One then computes (using very helpful tricks of Kodaira):

$$\Omega_{ij}(z) = \frac{1}{2\pi i} \log z \left(\begin{array}{c|c} S & 0 \\ \hline 0 & 0 \end{array}\right) - \left(\begin{array}{c|c} A(z) & B(z) \\ \hline {}^tB(z) & C(z) \end{array}\right)$$

where S is integral, positive definite and symmetric, and is obtained from the monodromy substitution for the cycle $|z| = 1$; where A, B, C are holomorphic in z at $z = 0$; and where $C(0)$ is the period matrix of the abelian part of $f^{-1}(0)$. This implies that $\Omega_{ij}(z) \longrightarrow C(0)$ in Satake's topology, when $z \to 0$.

§ 3. Compact moduli spaces for curves

Let M_g denote the moduli scheme for curves of genus g. Let

$$\Theta : M_g \longrightarrow \mathcal{V}_g$$

be the morphism which assigns to a curve its jacobian variety with its theta-polarization. From the work of Baily, Matsusaka, and Hoyt, it is known that Θ is an isomorphism of M_g with a locally closed subvariety of $\mathcal{V}_g$, which we also denote M_g'. The simplest approach to compactifying M_g' is to use its closure M_g^* in $\mathcal{V}_g^*$. This breaks up into two pieces

$$M_g' = (M_g^* \cap V_g) - M_g,$$

$$M_g'' = M_g^* - (M_g^* \cap V_g).$$

Matsusaka and Hoyt showed that M_g' is exactly the set of products of lower dimensional jacobian varieties. We have proven that $M_g'' = M_{g-1}^*$, so that

$$M_g^* = M_g \cup M_g' \cup M_{g-1} \cup M_{g-1}' \cup \text{-------} \cup M_0$$

($M_0 = \mathcal{V}_0$ is a single point).

The proof is based on two lemmas, and on the results of §2:

Lemma A: Let C be a curve and let $f : \mathfrak{X} \longrightarrow C$ be a family of curves of arithmetic genus g [i.e., f is proper and flat and its fibres $f^{-1}(P)$ are connected curves of arithmetic genus g]. Let $P_0 \in C$ and assume that $f^{-1}(P)$ is non-singular if $P \neq P_0$. Then there exists a diagram:

$$\begin{tikzcd} \mathfrak{X}' \arrow[r, "\pi'"] \arrow[d, "f'"'] & \mathfrak{X} \arrow[d, "f"] \\ C' \arrow[r, "\pi"'] & C \end{tikzcd}$$

where

1) C' is a curve and π is a finite morphism totally ramified over P_0 : let $P_0' = \pi^{-1}(P_0)$,
2) f' is a family of curves over C',
3) $\mathcal{X}' - f'^{-1}(P_0')$ is just the induced family of curves over $C' - P_0'$, i.e.

$$(C' - P_0') \times_C \mathcal{X} = \mathcal{X}' - f'^{-1}(P_0') ,$$

4) $f'^{-1}(P_0')$ is reduced and has only ordinary double points.

<u>Lemma B:</u> Let C be a curve and let

$$f : \mathcal{X} \to C$$

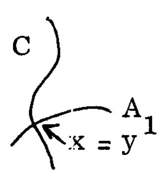
be a family of curves of arithmetic genus g such that each curve $f^{-1}(P)$ is reduced and has only ordinary double points. Then the set of generalized jacobian varieties of the curves $f^{-1}(P)$ forms a family of polarized semi-stable group varieties over C .

These lemmas give the inclusion $M_g'' \subset M_g^*$ directly; Lemma B and an easy construction of some actual families give the converse $M_g'' \supset M_g^*$.

Unfortunately, M_g^* is not a reasonable moduli space for curves: for example, let a point of M_g' correspond to

$$A_1 \times A_{g-1}$$

where A_1 is an elliptic curve, and A_{g-1} is the jacobian of a curve C of genus $g-1$. Let $x \in A_1$ and $y \in C$ be any points. Then $A_1 \times A_{g-1}$ is the generalized jacobian variety of the curve:



with an ordinary double point. In other words, the jacobian is independent of which y is chosen: i.e., Torelli's theorem is false for reducible curves. It is clearly necessary to blow up M_g'. This phenomenon is closely related to the fact, discovered by Bers and Ehrenpreis that the generic point of M_g' is not only singular on M_g^* : it is not even "almost non-singular" (= "Jungian" = "V-manifold"). In fact, Lemma A suggests

Definition:

A curve C of arithmetic genus g is stable if C is reduced and connected, has only ordinary double points, and has only a finite group of automorphisms.

It appears that the set of all stable curves is open and compact and is naturally isomorphic to the set of points of a compact analytic space with almost non-singular points: $\widetilde{M}_g^*$. It is still unknown whether $\widetilde{M}_g^*$ is a projective algebraic variety, although it is a Q-variety. There is a proper holomorphic map

$$\widetilde{M}_g^* \longrightarrow M_g^*$$

which is an isomorphism over the open subset M_g. One of the remarkable features of this case is that there are no semi-stable but not stable curves.

§4. Compact moduli spaces for abelian varieties: blown up

The preceding construction suggests the possibility of blowing up $\mathcal{V}_n^*$ so as to obtain a $\widetilde{\mathcal{V}}_n^*$ which corresponds to a moduli problem with a larger set of stable objects. We would like the stable points of $\widetilde{\mathcal{V}}_n^*$ to correspond to polarized compactifications of commutative group schemes X . One approach is to compactify the generalized jacobian varieties of curves C . Say C is irreducible and reduced: let J be the generalized jacobian of C . Then one has an isomorphism.

$$\left\{\begin{matrix}\text{points of}\\ J\end{matrix}\right\} = \left\{\begin{matrix}\text{invertible sheaves } L \text{ on } C\\ \text{such that } \chi(L) = \chi(\underline{O}_C)\end{matrix}\right\} .$$

We can prove that there is a projective scheme J* containing J as an open subset, and on which J acts, plus a natural isomorphism

$$\begin{matrix}\left\{\begin{matrix}\text{points of}\\ J\end{matrix}\right\} & \cong & \left\{\begin{matrix}\text{invertible sheaves } L \text{ on } C\\ \text{such that } \chi(L) = \chi(\underline{O}_C)\end{matrix}\right\}\\ \cap & & \cap \\ \left\{\begin{matrix}\text{points of}\\ J^*\end{matrix}\right\} & \cong & \left\{\begin{matrix}\text{rank 1, torsion-free sheaves } \mathcal{F} \text{ on } C\\ \text{such that } \chi(\mathcal{F}) = \chi(\underline{O}_C)\end{matrix}\right\}\end{matrix} .$$

Using this, we find an interesting $\widetilde{\mathcal{V}}_2^*$, in which only one point is still mysterious: that is the point which is the image under Θ of the curve of genus 2 depicted below:

SEMINAR ON ÉTALE COHOMOLOGY OF NUMBER FIELDS

by

Michael Artin & Jean-Louis Verdier

1.)

Notation (1.1) k = a number field.

A = integers in k.

X = Spec A.

$U \subset X$ a nonempty Zariski-open subset.

The etale cohomology of U with values in the multiplicative group $\mathbb{G}_m$ can be described by class field theory as follows:

Denote by

$$i: \operatorname{Spec} k \longrightarrow U$$

the map. One has the usual exact sequence

(1.2) $$0 \longrightarrow (\mathbb{G}_m)_U \longrightarrow i_*(\mathbb{G}_m)_k \longrightarrow D \longrightarrow 0$$

where

$$D = \bigoplus_{\substack{x \text{ closed} \\ \text{in } U}} (\mathbb{Z})_x$$

is the sheaf of Cartier divisors on U. Now by local class field theory,

(1.3) $$R^q i_* \mathbb{G}_m = 0, \quad q > 0, \qquad \text{i.e.,}$$

$$H^q(U, i_*\mathbb{G}_m) \approx H^q(\operatorname{Spec} k, \mathbb{G}_m), \quad \text{all } q.$$

Taking into account the vanishing of certain groups, the exact cohomology sequence of (1.2) yields the exact sequences

(1.4) $$0 \longrightarrow \mathbb{G}_m(U) \longrightarrow k^* \longrightarrow \bigoplus_x (\mathbb{Z}) \longrightarrow \operatorname{Pic} U \longrightarrow 0,$$

$$0 \longrightarrow H^2(U, \mathbb{G}_m) \longrightarrow \operatorname{Br} k \xrightarrow{\phi} \bigoplus_x (\mathbb{Q}/\mathbb{Z}) \longrightarrow H^3(U, \mathbb{G}_m) \longrightarrow 0$$

where $\mathrm{Br}\, k = H^2(\mathrm{Spec}\ k, \mathbb{G}_m)$ and $\mathbb{Q}/\mathbb{Z} = H^2(k(x), \mathbb{Z})$. The map ϕ is the one given by class field theory.

Corollary (1.5): If k is totally imaginary then

$$H^q(X, \mathbb{G}_m) = \begin{cases} A^* & , \ q = 0, \\ \mathrm{Pic}\ X & , \ q = 1, \\ 0 & , \ q = 2, \\ \mathbb{Q}/\mathbb{Z} & , \ q = 3. \end{cases}$$

Theorem (1.6): Suppose $p \neq 2$ or that k is totally imaginary. Then $\mathrm{cd}_p X = 3$ and $\mathrm{cd}_p U = 2$ if $U \neq X$.

2.)

In this section we denote by $f: X \longrightarrow \mathrm{Spec}\ \mathbb{Z}$ a scheme of finite type. Because of "Artin-Schreier" theory, one can show that for a scheme Y of characteristic p

$$(2.1) \qquad \mathrm{cd}_p Y \leq \mathrm{cdqc}\ Y + 1 \qquad (p = \mathrm{char}\ Y)$$

where $\mathrm{cdqc}\ Y = \sup[q \mid H^q(Y, F) \neq 0$ for some quasi-coherent sheaf F on $Y]$. Using this and dimension theory for fields, one obtains

Theorem (2.2): $\mathrm{cd}_p X \leq 2 \dim X + 1$ if $p \neq 2$.

The rest of this section is devoted to 2-cohomology.

Notation (2.3): X_∞ = space of closed points of $X \otimes_{\mathbb{Z}} \mathbb{R}$ with the real topology

$= X(\mathbb{C})/G$, where $X(\mathbb{C})$ is the space of points of X with values in $\mathbb{C}$, with the usual topology, and where $G = \mathbb{Z}/2$ operates by complex conjugation.

$X(\mathbb{R})$ = real locus of X, which is a closed subspace of X_∞.

$\bar{X}$ = the topological space whose underlying set is $X \amalg X_\infty$ with the topology whose open sets are pairs (X', U) where X' is a Zariski open set in X, and U is an open subset of X'_∞.

Actually, we will work with the following étale topology on $\bar{X}$: The category of open sets are pairs $(f: X' \longrightarrow X, U)$ consisting of a morphism of schemes f and an open subset U of X'_∞ having the following properties:

(a) f is étale.

(b) In the map $g: U \longrightarrow X_\infty$ induced by f, $g(u) \in X(\mathbb{R}) \Rightarrow u \in X'(\mathbb{R})$.

A map $(f_1, U_1) \longrightarrow (f_2, U_2)$ is a map $X'_1 \longrightarrow X'_2$ commuting with the structure maps and such that under the induced map $X'_{1\infty} \longrightarrow X'_{2\infty}$, U_1 is carried into U_2. A family of maps with range (f, U) is a covering iff (X', U) is the union of the images.

For this topology, there are morphisms $X_{et} \xrightarrow{j} \bar{X}_{et}$ and $X_\infty \xrightarrow{i} \bar{X}_{et}$ where X_∞ is taken with the topology of local isomorphisms. The map j is formally an open immersion and i is its closed complement. The derived functors $R^q j_* F$ for a sheaf F on X_{et} are 2-torsion sheaves concentrated on the real locus $X(\mathbb{R})$, $q > 0$.

Theorem (2.4): Let $X = \operatorname{Spec} A$ be the ring of integers in a number field, and set $(\mathbb{G}_m)_{\bar{X}} = j_*(\mathbb{G}_m)_X$. Then

$$H^q(\bar{X}, \mathbb{G}_m) = \begin{cases} A^*, & q = 0, \\ \operatorname{Pic} X, & q = 1, \\ 0, & q = 2, \\ \mathbb{Q}/\mathbb{Z}, & q = 3, \\ 0, & q > 3 \end{cases}.$$

(Slight variations in dimensions $0, 1$ could be obtained by insisting that a unit of $\mathbb{G}_m$ be positive at a real prime.) The above is an easy consequence of the following theorem:

Theorem (Tate): Let k be a number field and F a sheaf on $\operatorname{Spec} k$. Then

$$H^q(\operatorname{Spec} k, F) \longrightarrow H^q(\operatorname{Spec}(k \otimes_{\mathbb{Z}} \mathbb{R}), F_{\mathbb{R}})$$

is surjective, $q=2$, and bijective, $q > 2$. Here $F_{\mathbb{R}}$ denotes the induced sheaf.

Theorem (2.5): Let F be a sheaf on $\bar{X}$ whose restriction to X is a noetherian torsion sheaf. Then $H^q(\bar{X}, F) = 0$ for $q > 2 \dim X + 1$.

Corollary (2.6): (a) $H^q(X, F) \xrightarrow{\sim} H^q(X \otimes_{\mathbb{Z}} \mathbb{R}, F_{\mathbb{R}})$ for $q > 2\dim X + 1$.

(b) $cd_2 X < \infty \Leftrightarrow cd_2 X \leq 2 \dim X + 1 \Leftrightarrow X(\mathbb{R}) = \emptyset$.

(c) for a field K of finite type, $cd_2 K = \infty$ iff K is a real field.

(Part (c) is also an easy consequence of a general result of Serre.)

3)

We use the notations of section 1. Let $F^{\cdot}$ be a complex of sheaves over X whose cohomology is bounded (i.e., $H^q(F^{\cdot}) = 0$ for q sufficiently large) and such that $H^q(F^{\cdot})$ is a noetherian torsion sheaf for all q.

We denote by $\underline{\underline{H}}^q(X, F^{\cdot})$ the hypercohomology of X into $F^{\cdot}$ and by $\underline{\underline{\mathrm{Ext}}}^q(X; F^{\cdot}, G_m)$ the global hyper-Ext on X. For any q those groups are finite commutative groups and for q sufficiently large they are equal to zero.

For any prime integer p and for any finite commutative group M we denote by M_p the p-primary component of M.

Theorem (3.1): The Yoneda product

$$(*)_p \quad \underline{\underline{H}}^q(X, F^{\cdot})_p \times \underline{\underline{\mathrm{Ext}}}^{3-q}(X; F^{\cdot}, G_m)_p \longrightarrow H^3(X, G_m)_p \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p$$

is a perfect duality for $p \neq 2$. If k is a totally imaginary field, the pairing $(*)_2$ is also a perfect duality.

Let now U be an open subscheme of X and $F^{\cdot}$ a complex of sheaves on U satisfying the same conditions as in the beginning of the section. The complex $F^{\cdot}_U$ will be the complex of sheaves on X obtained by extending the complex $F^{\cdot}$ by zero. We define $\underline{\underline{H}}^2_c(U, F^{\cdot})$ (hypercohomology with compact support on U) by the equality:

$$\underline{\underline{H}}^q_c(U, F^{\cdot}) = \underline{\underline{H}}^q(X, F^{\cdot}_U).$$

Similarly, given any complex $G^{\cdot}$ of sheaves on U (whose cohomology is bounded), we define the groups $\underline{\underline{\mathrm{Ext}}}^q_c(U; F^{\cdot}, G^{\cdot})$ (Hyper-Ext with compact support) in the following way: First we take an injective resolution $I(G^{\cdot})$ of $G^{\cdot}$ (i.e., a morphism of complexes $\rho : G^{\cdot} \longrightarrow I(G^{\cdot})$ into a complex whose objects are injective sheaves which induces an isomorphism on the sheaves of cohomology). Then we define the complex of sheaves on U : $\underline{\mathrm{Rhom}}(F^{\cdot}, I(G^{\cdot}))$ to be the single complex of sheaves on U of sheaf homomorphism of $F^{\cdot}$ into $I(G^{\cdot})$. Then we define $\underline{\underline{\mathrm{Ext}}}_c^q(U;F^{\cdot},G^{\cdot})$ by the equality:

$$\underline{\underline{\mathrm{Ext}}}_c^q(U;F^{\cdot},G^{\cdot}) = \underline{\underline{H}}^q(X, \underline{\mathrm{Rhom}}(F^{\cdot}, I(G^{\cdot}))_U).$$

When the complex $G^{\cdot}$ is the single sheaf $\mathbb{G}_m$, the complex $\underline{\mathrm{Rhom}}(F^{\cdot}, I(\mathbb{G}_m))$ will be denoted by $D(F^{\cdot})$.

As an immediate corollary of the theorem 3.1, we obtain:

Corollary 3.2: The Yoneda product

$$\underline{\underline{H}}_c^q(U,F^{\cdot})_p \times \underline{\underline{\mathrm{Ext}}}^{3-q}(U;F^{\cdot},\mathbb{G}_m)_p \longrightarrow \underline{\underline{H}}_c^3(U,\mathbb{G}_m)_p \xrightarrow{\sim} Q_p/\mathbb{Z}_p$$

is a perfect duality for any prime p different from 2. If k is totally imaginary, it is also a perfect duality for p = 2.

Let us denote by $\triangle$ the canonical morphism of complexes

$$\triangle : F^{\cdot} \longrightarrow D(D(F^{\cdot})).$$

Theorem 3.3: When the torsion of the cohomology sheaves of $F^{\cdot}$ is prime to the residual characteristics of U, the morphism $\triangle$ induces an isomorphism on the sheaves of cohomology.

As an immediate corollary of the theorem 3.3, we obtain:

Corollary 3.4: The Yoneda product

$$\underline{\underline{H}}^q(U,F^{\cdot})_p \times \underline{\underline{\mathrm{Ext}}}_c^{3-q}(U;F^{\cdot},\mathbb{G}_m)_p \longrightarrow \underline{\underline{H}}_c^3(U,\mathbb{G}_m)_p \xrightarrow{\sim} Q_p/\mathbb{Z}_p$$

is a perfect duality for any complex $F^{\cdot}$ whose torsion of cohomology sheaves is prime to the residual characteristics of U and for any prime p different from 2. As usual, when k is a totally imaginary field, the restriction $p \neq 2$ can be omitted.

ELLIPTIC CURVES AND FORMAL GROUPS

Lubin, Serre, Tate

1. Serre discussed his results on the action of Galois groups on the points of finite order on elliptic curves over number fields and local fields [4]. The local results in case of non-degenerate reduction can be obtained by methods to be discussed in this seminar.

2. Lubin discussed results from [2] on the endomorphism rings of formal Lie groups on one parameter over $\mathfrak{p}$-adic integer rings. If A is a commutative ring with identity, <u>a one-parameter formal Lie group over A</u> is a power series $F(x, y) \in A[[x, y]]$ such that

1. $F(x, y) \equiv x + y \mod \deg 2$
2. $F(F(x, y), z) = F(x, F(y, z))$
3. $F(x, y) = F(y, x)$

If F and G are two such formal groups an <u>A-homomorphism of F into G</u> is a power series $f(x) \in A[[x]]$ such that f has no constant term and $f(F(x, y)) = G(fx, fy)$.

The set of all such homomorphisms is called $\mathrm{Hom}_A(F, G)$ and is an abelian group under the addition $(f + g)(x) = G(fx, gx)$; the group $\mathrm{End}_A(F) = \mathrm{Hom}_A(F, F)$ is a ring. If $f \in \mathrm{End}_A(F)$, we denote by $c(f)$ its first-degree coefficient.

<u>Proposition</u>. <u>If</u> A <u>is an integral domain of characteristic zero, and</u> F <u>a formal group over</u> A, <u>the map</u>

$$c : \mathrm{End}_A(F) \to A$$

<u>is an injective ring-homomorphism</u>.

In the case we are interested in, where A is a $\mathfrak{p}$-adic integer ring, i.e., a complete rank-one valuation ring of characteristic zero, with residue class field of characteristic $p > 0$, $c(\mathrm{End}_A(F))$ is closed in A so that the endomorphism ring always contains $\mathbb{Z}_p$, the p-adic integers.

<u>Proposition</u>. <u>If</u> F <u>is a formal Lie group defined over the $\mathfrak{p}$-adic integer ring</u> $\mathfrak{o}$, <u>and</u> F^*, <u>the formal group defined over</u> $k = \mathfrak{o}/\mathfrak{p}$ <u>by reducing all the coefficients of</u> F <u>modulo</u> $\mathfrak{p}$, <u>is such that</u> F^* <u>is not k-isomorphic to the additive formal group</u> $x + y$, <u>then</u> $\mathrm{End}_{\mathfrak{o}}(F)$ <u>is injected into</u> $\mathrm{End}_k(F^*)$ <u>by the reduction map</u> $f \mapsto f^*$.

We know that over the algebraic closure K of k, $\mathrm{End}_k(F^*)$ is isomorphic to the unique maximal order in the central division algebra D_h of rank h^2 and invariant $1/h$ over $\mathbb{Q}_p$. Here h is the height of F^* as defined by Lazard [1].

Thus since $\mathrm{End}_{\mathcal{O}}(F)$ is a commutative subring of $\mathrm{End}_K(F^*)$, its fraction field must be isomorphic to a subfield of D_h and so the degree of this field over $\mathbb{Q}_p$ must divide h.

A consequence of this is that if F is defined over $\mathcal{O}$, there is a finite extension $\mathcal{O}'$ of $\mathcal{O}$ such that for any larger $\mathcal{O}''$, $\mathrm{End}_{\mathcal{O}''}(F) = \mathrm{End}_{\mathcal{O}'}(F)$. We call this $\mathrm{End}_{\mathcal{O}'}(F)$ the absolute endomorphism ring of F, and denote it $\mathrm{End}(F)$.

If F is defined over a $\mathfrak{p}$-adic integer ring $\mathcal{O}$, the height of F is defined to be the height of F^*, the formal group defined over $k = \mathcal{O}/\mathfrak{p}$.

If F is of height $h < \infty$ over $\mathcal{O}$, F is <u>full</u> if

1. $\mathrm{End}(F)$ is integrally closed in its fraction field K.
2. $[K : \mathbb{Q}_p] = h$.

It turns out that for every local field K there is a full formal group whose endomorphism ring is the ring of integers K.

3. Lubin discussed results from [3], and some other conjectures about points of finite order on formal groups.

If F is a formal group of height $h < \infty$ defined over $\mathcal{O}$, and $\mathcal{C}$ is the ring of integers in any complete extension $\mathcal{L}$ of L = the fraction field of $\mathcal{O}$, and if $\mathcal{P}$ is the maximal ideal of $\mathcal{C}$, then $\mathcal{P}$ can be made into a group by means of $: \alpha + \beta = F(\alpha, \beta)$. Clearly the only elements of this group of finite order are of order p^n for some n: if we call $[\lambda]_F$ the endomorphism of F corresponding to the p-adic integer λ, then assuming that we have $\alpha \in \mathcal{P}$ such that $[m]_F(\alpha) = 0$ for $p \nmid m$; since $[\frac{1}{m}]_F \in \mathrm{End}_{\mathcal{O}}(F)$, $([\frac{1}{m}]_F \circ [m]_F)(\alpha) = 0$ and so $\alpha = 0$.

Now since F is of height h, the endomorphism $[p]_F$ is a power series whose first unit coefficient is in degree p^h. Thus the first unit coefficient of $[p^r]_F(x)$ is in degree p^{rh}. And a Weierstrass preparation type argument shows that $[p^r]_F(x) = P(x) \cdot U(x)$ where $P(x)$ is a monic polynomial of degree p^{rh} such that all coefficients of degree less than p^{rh} are in $\mathfrak{p}$, and where $U(x)$ is a power series with unit constant term. Thus in a sufficiently large $\mathcal{C}$, there are exactly p^{rh} elements $\alpha \in \mathcal{P}$ such that $[p^r]_F(\alpha) = 0$.

We can form the "Tate group" of F:

$T(F) = \varprojlim_n T_{p^n}(F)$ where $T_{p^n}(F)$ is the group of all α in the algebraic closure of L such that $[p^n]_F(\alpha) = 0$; the projective limit is taken with respect to the maps $[p^{m-n}]_F : T_{p^m} \to T_{p^n}$ $(m > n)$.

Then $T(F)$ is a free $\mathbb{Z}_p$-module of rank h. It is also an $\mathrm{End}_{\mathcal{O}}(F)$-module. Let us assume that $c(\mathrm{End}(F)) \subset \mathcal{O}$ so that K, the fraction-field of $c(\mathrm{End}(F))$, is a subfield of L. Call $\mathcal{L}$ the field gotten by adjoining to L all roots of $[p^n]_F$ (all n). Then $G = \mathcal{G}(\mathcal{L}/L)$ has a faithful representation $G \hookrightarrow \mathrm{End}_{\mathbb{Z}_p}(T(F)) \cong GL(h, \mathbb{Z}_p)$ $\subset GL(h, \mathbb{Q}_p)$ but also the action of G on $T(F)$ commutes with $\mathrm{End}(F)$ so $T(F) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is an $\mathrm{End}(F) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong K$-module of rank $s = \frac{h}{r}$ where r is the $\mathbb{Z}_p$-rank of $\mathrm{End}(F)$. One may ask whether G is open in $GL(s, K)$, or, at any rate, whether the commuting algebra of G in $\mathrm{End}(T(F)) \otimes \mathbb{Q}_p$ is reduced to K. We have no indication of the truth or falsity of this, except in the case $s = 1$, where it is true, and can be used to give an explicit reciprocity law in local class field theory in the following way:

As mentioned before, for each finite extension K of $\mathbb{Q}_p$, with ring of integers $\mathfrak{o}$, there is a full formal group F defined over $\mathfrak{o}$ whose absolute endomorphism ring is isomorphic to $\mathfrak{o}$. Then $T(F)$ is a free $\mathfrak{o}$-module of rank 1 and so $G = \mathcal{G}(\mathcal{L}/K) \hookrightarrow GL(1, \mathfrak{o}) = \mathfrak{o}^*$. A simple counting argument shows that in fact this map is onto. The field $\mathcal{L}$ is a totally ramified abelian extension of K and in fact a maximal such, and the action of $\mathfrak{o}^*$ on $\mathcal{L}$ given by the above isomorphism turns out to be the inverse of that furnished by the reciprocity law of local class-field theory: specifically, if $[p^n](\alpha) = 0$ for some n, and $u \in \mathfrak{o}^*$,

$$(u, \mathcal{L}/K)(\alpha) = [u^{-1}]_F(\alpha).$$

By patching this together with the Frobenius mapping on the maximal unramified extension of K, we get an explicit reciprocity formula for the maximal abelian extension of K.

4. Lubin discussed unpublished results of Lubin-Tate on moduli of formal groups. Let Φ be a formal group of height $h < \infty$ defined over the residue class field $k = \mathfrak{o}/\mathfrak{p}$. Such a Φ is k-isomorphic to one satisfying $\Phi(x, y) \equiv x + y \pmod{\deg p^h}$, and we will assume this condition satisfied for the sake of convenience. Let $t = (t_1, \ldots, t_{h-1})$ be a family of $h-1$ independent transcendentals. By methods of Lazard [1] it is easy to construct a formal group $\Gamma(t_1, \ldots, t_{h-1})(x, y)$ with coefficients in the polynomial ring $\mathfrak{o}[t_1, \ldots, t_{h-1}]$ such that

(i) $\Gamma^*(0, \ldots, 0)(x, y) = \Phi(x, y)$

(ii) $\Gamma(0, \ldots, 0, t_i, \ldots, t_{h-1})(x, y) \equiv x + y + t_i C_{p^i}(x, y) \pmod{\deg p^i + 1}$.

Choose such a Γ. Let A be a local $\mathfrak{o}$-algebra with maximal ideal M. If we specialize the t_i to elements $\alpha_i \in M$, we obtain a group law $\Gamma(\alpha)(x, y)$ defined over A which reduces mod M to Φ, i.e. such that $\Phi = (\Gamma(\alpha))^*$. (Here we are identifying $k = \mathfrak{o}/\mathfrak{p}$

with its canonical image in A/M).

Theorem: Suppose A is separated and complete for the M-adic topology. Let F be a formal group over A such that $\Phi = F^*$. Then there exist $\alpha_i \in M$, $1 \leq i \leq h-1$, and an A-isomorphism $\phi: F \simeq \Gamma(\alpha)$ such that $\phi^* =$ identity. Moreover, the point $\alpha = (\alpha_1, \ldots, \alpha_{h-1})$ and ϕ are unique.

In other words, the functor which associates with each complete local $\mathfrak{o}$-algebra A the set of isomorphism classes of formal groups F over A reducing to Φ mod M (allowable isomorphisms being those A-isomorphisms reducing to identity mod M) is representable by the "universal" group law $\Gamma(t)$ over the algebra $\mathfrak{o}[[t_1, \ldots, t_{h-1}]]$. As usual, there results an operation of Aut Φ on $\mathfrak{o}[[t]]$, whose study should be interesting. In case $h = 2$ we have used it to construct an elliptic curve E over $\mathfrak{o}$ whose formal group has complex multiplication, although E does not.

5. Tate discussed a mixed group-sheaf cohomology. Let S be a ground scheme, X a group scheme over S, and B a commutative group scheme over S. Suppose X operates on B in an evident sense. Let $\mathfrak{U}$ be an open covering of X. With the aid of the group law $X \times X \to X$, one can associate with $\mathfrak{U}$ a certain open cover $\mathfrak{U}^{(p)}$ of $X^p = X \times X \times \ldots \times X$ (p times), for each p. One can then define a double complex $C^{\cdot\cdot}(\mathfrak{U}, X, B)$ in which an element of $C^{p,q}$ is a family of morphisms from the intersections of $(q+1)$ open sets in the covering $\mathfrak{U}^{(p)}$ into B. The differentiation $C^{p,q} \to C^{p,q+1}$ is as in the Čech sheaf cohomology, while the differentiation $C^{p,q} \to C^{p+1,q}$ is defined by formulas as in standard inhomogeneous complex in the ordinary cohomology of groups. Passing to the associated single complex and cohomology we get groups $H^n(\mathfrak{U}, X, B)$. For example, $H^2(\mathfrak{U}, X, B)$ describes the group-scheme extensions of X by B which, as fiber spaces, are trivial on the covering $\mathfrak{U}$. Passing to the limit over $\mathfrak{U}$, we get groups $H^n(X, B)$.

6. Tate discussed results of Serre-Tate on the raising of abelian varieties from characteristic p, the main idea being that to raise A is equivalent to raising consistently the finite subschemes $\mathrm{Ker}(A \xrightarrow{p^n} A)$ for all n. Let R be an Artinian local ring with residue field $k = R/\mathfrak{m}$. Let I be an ideal in $\mathfrak{m}$ such that $\mathfrak{m} I = 0$. Put $R' = R/I$. We wish to "raise" things from R' to R.

(i) Raising homomorphisms of groups. Let B be a group scheme smooth over R, and let X be a group scheme flat over R. Assume X and B are commutative for simplicity. Let

$$B' = B \otimes_R R', \quad X' = X \otimes_R R', \quad \widetilde{B} = B \otimes_R k, \text{ etc.}$$

Let $t(\widetilde{B})$ be the tangent space to the origin on $\widetilde{B}$. The tensor product $t(\widetilde{B}) \otimes I$ is a finite dimensional vector space over k. Let $W(t(\widetilde{B}) \otimes I)$ denote the corresponding group scheme over k, isomorphic to the direct product of $(\dim \widetilde{B})(\dim_k I)$ copies of the additive group $\mathbb{G}_a$.

<u>Theorem</u>. <u>There is an exact sequence</u>

$$0 \to \mathrm{Hom}_k(\widetilde{X}, W(t(\widetilde{B}) \otimes I)) \to \mathrm{Hom}_R(X, B) \to \mathrm{Hom}_{R'}(X', B') \xrightarrow{\delta} H^2(\widetilde{X}, W(t(\widetilde{B}) \otimes I)).$$

Here the Homs are <u>group</u> homomorphisms. The H^2 is that defined in the preceding section, and the image of δ is contained in the symmetric part of H^2, and hence can be viewed as in $\mathrm{Ext}^1(\widetilde{X}, W)$. The theorem is proved by means of an exact sequence of complexes as in § 5

$$0 \to C^{\cdot\cdot}(\mathcal{U}, \widetilde{X}, W) \to C^{\cdot\cdot}(\mathcal{U}, X, B) \to C^{\cdot\cdot}(\mathcal{U}, X', B') \to 0,$$

where $\mathcal{U}$ is an affine open covering of X. The exactness follows from the fact that on an affine set, a morphism $X' \to B'$ can be raised to $X \to B$.

Of course the interesting point is the δ: the obstruction to raising a homomorphism of commutative groups lies in $\mathrm{Ext}(\widetilde{X}, W)$. A geometric description of that extension could certainly be given (and might enable one to avoid the mixed group-sheaf cohomology of §5). It would also be interesting to examine the relations between this and the group extensions given by Greenberg's functor (assuming k perfect); if $I = m$, it seems that Greenberg's extension is obtained from the other by a suitable power of Frobenius.

(ii) <u>Lifting abelian varieties</u>. Suppose now that k is of characteristic $p \neq 0$. The main theorem can be formulated by saying that there is an <u>equivalence of categories</u> $C_1 \to C_2$, where:

(C_1) is the category of abelian schemes over R.

(C_2) is the category of pairs (Φ, X), where Φ is an abelian scheme over k, and where X is a raising to R of Φ^*. For this to make sense, we must say what A^* is if A is an abelian scheme over R (or k):

$$A^* = \lim_{n \to \infty} A_{p^n}, \text{ where } A_{p^n} = \mathrm{Ker}(p^n : A \to A).$$

Of course the kernel A_{p^n} is taken as a group scheme (finite and flat over R (or k)). Concerning A^* one considers it as an ind-object; the notion of a raising to R of Φ^* is therefore equivalent to that of a sequence of raisings of the Φ_{p^n} to group schemes X_n flat over R, together with injections $X_n \to X_{n+1}$ raising the canonical inclusions $\Phi_{p^n} \subset \Phi_{p^{n+1}}$. In what follows we shall pretend that A^* (or Φ^*) is a true group scheme - it is clear that that will not lead to serious worries.

The functor $C_1 \to C_2$ is clear; it associates with each abelian scheme A over R the pair $(\tilde{A}, A^*)$ where $\tilde{A}$ is the reduction of $A \pmod{m}$, which is an abelian variety over k. Clearly, A^* is a raising of $(\tilde{A})^*$. The marvellous thing is that it is an equivalence of categories! In other words, if one knows the reduction $\tilde{A}$ of an abelian scheme A, all that is lacking to determine A is a raising of the ind-group scheme $\tilde{A}^*$, which is quite an innocent thing (see below).

The proof of the theorem which was sketched in the seminar used the exact sequence of (i) above together with known facts about the existence of raisings of abelian schemes. However, with better foundations, the theorem should result formally from:

Lemma. <u>One has</u> $\mathrm{Ext}^i(\Phi, \mathbb{G}_a) \xrightarrow{\sim} \mathrm{Ext}^i(\Phi^*, \mathbb{G}_a)$ <u>for all</u> i.

(In fact, these groups are zero for $i \neq 1$, and for $i = 1$, they are k-vector spaces of dimension $\dim A$.) The lemma would result from the fact that Φ / Φ^* is uniquely divisible by p, hence all its Exts with $\mathbb{G}_a$ are zero.

7. Serre discussed applications of the preceding.

(iii) <u>The case where</u> Φ <u>has no point of order</u> p. In this case one can identify Φ^* with the <u>formal group</u> attached to Φ. Thus, to raise Φ is the same as to raise its formal group. In case $\dim \Phi = 1$ (Φ an elliptic curve with Hasse inv. $= 0$) the raising of the formal group has been discussed by Lubin in section 4 above.

(iv) <u>The case where</u> Φ <u>has the maximum number of points of order</u> p. [This is the case which Serre has treated previously (unpublished) by the method of Greenberg. The present theory gives new proofs, more satisfying in certain respects.] We suppose k <u>perfect</u> (this seems essential, and not only due to our natural taste for Galois theory). Let $n = \dim \Phi$. The hypothesis made on Φ amounts to saying that Φ_p is the direct sum of an étale k-group of order p^n and an infinitesimal k-group of "order" p^n. The first is a $(\mathbb{Z}/p\mathbb{Z})^n$ twisted by Galois, and the second a $(\mu_p)^n$ twisted analogously. More generally one has a canonical decomposition:

$$\Phi^* = \Phi^*_m + \Phi^*_{et}.$$

Now it is clear that Φ^*_{et} has a unique lifting to R (Hensel). It is the same (for example by Cartier duality or by the results of Dieudonné) for Φ^*_m. One sees therefore immediately <u>that there is a canonical way to raise</u> Φ^*, namely the direct sum of the raisings of Φ^*_m and Φ^*_{et}, and there results, by the general theory a <u>canonical raising of the abelian variety</u> Φ. It is easy to see that one even obtains in this way a <u>functor</u> from the category of the Φ to the category C_1, a functor which is inverse to the reduction functor (N.B. this inverse is defined only on the Φ having the maximum number of points of order p.). If one passes to the limit over R, one finds <u>a priori</u> a <u>formal abelian scheme</u> raising Φ canonically, but Mumford explained to us how, using the canonicalness, one can prove that it is in reality an abelian scheme.

Before discussing the canonical raisings in more detail, let us say a word about the other raisings. We suppose for simplicity that k is algebraically closed. It is almost evident that each lifting of Φ^*, call it A^*, is an extension.

$$0 \to A^*_m \to A^* \to A^*_{ét} \to 0$$

where A^*_m and $A^*_{ét}$ are the canonical raisings of Φ^*_m and Φ^*_{et}. To suppose k algebraically closed allows us to identify these latter groups with the groups $(\mathbb{G}_m\text{-formal})^n$, and $(\mathbb{Q}_p/\mathbb{Z}_p)^n$, these groups being taken over R in the obvious sense. It is then an exercise to show that an R-extension of $\mathbb{Q}_p/\mathbb{Z}_p$ by $\mathbb{G}_m$-formal is characterized by an element of the group $R^*_1 = 1+\mathfrak{m}$, the multiplicative group of elements of R congruent to 1 modulo the maximal ideal $\mathfrak{m}$.

Passing to the limit over R, one sees that this result continues to hold if one is over a complete noetherian local ring R with residue field k. Of course one is no longer sure that one has true abelian schemes, but in any case, one has formal schemes. Therefore one can say that the formal variety of moduli has as its points the systems of n^2 Einseinheiten; it has moreover a canonical group structure.

The abelian schemes, or formal schemes, whose moduli (in the preceding sense) are of <u>finite order</u> deserve the name <u>quasi-canonical</u>. In case R is a discrete valuation ring, such a scheme is isogenous to a canonical scheme; the situation is not clear in the general case.

Continuing to assume R a discrete valuation ring of characteristic zero, there is a simple characterization of the quasi-canonical schemes: there are those for which the module $V_p = T_p \otimes \mathbb{Q}_p$ <u>splits</u> as a module over the p-adic Lie algebra of the Galois group. In this way one arrives at a justification of theorem 1, page 9, of [4] .

8. Serre discussed the canonical raising of elliptic curves. The problem considered is the following. Let k be perfect, and let E be an elliptic curve with invariant $j \in k$ and with Hasse invariant $\neq 0$ (i.e., having the maximum number of points of order p); by the preceding discussion, there is a canonical lifting of E to the ring W(k) of Witt vectors. The j of that lifting is therefore a function

$$\theta : k - \mathrm{Ker}(\mathrm{Hasse}) \to W(k)$$

How does one calculate θ ?

Let s be the Frobenius automorphism of W(k), given by $(x_0, x_1, \ldots) \mapsto (x_0^p, x_1^p, \ldots)$. Let $T_p(j, j')$ be the classical equation relating the modular invariants of two elliptic curves having an isogeny of degree between themselves, an equation with coefficients in $\mathbb{Z}$, symmetric in j, j'.

<u>Theorem (i)</u> <u>Let</u> $\lambda \in k - \mathrm{Ker}\,(\mathrm{Hasse})$, <u>and let</u> $x = \theta(\lambda) \in W(k)$. <u>One has</u>

(*) $\qquad T_p(x, s(x)) = 0$, and $x = \lambda \pmod{p}$

(ii) If $\lambda \in k - \mathbb{F}_{p^2}$, the system (*) has a unique solution.

(Combining (i) and (ii) one sees therefore that (*) characterizes $x = \theta(\lambda)$, provided that $\lambda \notin \mathbb{F}_{p^2}$).

To prove (i) one applies the functor "canonical raising" to the Frobenius isogeny: $E \to E^{(p)}$. The canonical raising of $E^{(p)}$ is obtained from that of E by applying the automorphism s. Its modular invariant $s(x)$ is therefore related to the invariant x of the raising of E by the equation $T_p(x, s(x)) = 0$, hence (i). The assertion (ii) is proved in a standard way by successive approximations. The hypothesis $\lambda \notin \mathbb{F}_{p^2}$ intervenes in order to be sure that a certain partial derivative of T_p does not vanish.

Just for fun, here is a numerical example: for $p = 2$, $\lambda = 1$, the canonical raising $\theta(\lambda)$ is equal to $-3^3 5^3$.

References

[1] M. Lazard. <u>Sur les groupes de Lie formels à un paramètre</u>. Bull. Soc. Math. France <u>83</u> (1955), p. 251-274.

[2] J. Lubin. <u>One-parameter formal Lie groups over $\mathfrak{p}$-adic integer rings</u>. Annals of Math. to appear.

[3] J. Lubin and J. Tate. <u>Formal complex multiplication in local fields</u>. Annals of Math. to appear.

[4] J.P. Serre. <u>Groupes de Lie ℓ-adiques attachés aux courbes elliptiques</u>. Colloque de Clermont-Ferrand, April, 1964.

FAMILY OF ABELIAN VARIETIES AND NUMBER THEORY

PART I

by

Michio Kuga

§1. Let G be a connected real semi-simple Lie group, and K be a maximal compact subgroup of G; so that $X = G/K$ is a symmetric space. Furthermore, we assume that X has a G- invariant complex structure. Denote by $\nu : G \to X$ the natural mapping. Let Γ be a discrete subgroup of G containing no finite subgroup except $\{1\}$, and such that $\Gamma \backslash G$ is compact. Then $U = \Gamma \backslash X = \Gamma \backslash G/K$ is a projective non-singular algebraic variety. Let $\rho : G \longrightarrow GL(N, R)$ be a representation of G, such that $\rho(\gamma) \in SL(N, Z)$ for all $\gamma \in \Gamma$. Then for every $\gamma \in \Gamma$, the matrix $\rho(\gamma)$ induces an automorphism $\bar{\rho}(\gamma)$ of the torus $F = R^n/Z^n$. Let us make Γ operate on the product space $X \times F$ by the rule: $X \times F \ni (x, u) \rightsquigarrow \gamma(x, u) = (\gamma(x), \bar{\rho}(\gamma) u) \in X \times F$ (for $\gamma \in \Gamma$). This operation is properly discontinuous, with no fixed point for $\gamma \neq 1$, and $V = \Gamma \backslash (X \times F)$ is a compact manifold. It is easy to find the projection map π of V onto U which makes the following diagram commutative:

$$\begin{tikzcd}
V \arrow[d, "\pi"'] & & X \times F \arrow[ll, "\text{the natural map} = \tilde{p}"'] \arrow[d, "\tilde{\pi}"] & \ni & (x, u) \arrow[d, maps to] \\
U & & X \arrow[ll, "\text{the natural map} = p"] & \ni & x
\end{tikzcd}$$

This construction shows that $V \xrightarrow{\pi} U$ is a fibre bundle over U such that: (1) the typical fibre is the torus, F; (2) the structure group is Γ; (3) the action of Γ on F is $\bar{\rho}$; (4) it is associated with the universal covering $X \xrightarrow{p} U$.

Let us assume furthermore, that there exists a non-singular integral alternating $N \times N$ matrix B such that ${}^t\rho(g)\, B\, \rho(g) = B$ for all $g \in G$. This means that ρ is a homomorphism of G into the symplectic group $Sp(B) = \{ m \in GL(N, R);\ {}^t m\, B\, m = B \}$ ($\cong Sp(N/2, R)$) of B. For such a matrix B we can find a positive definite real symmetric matrix S such that: (5) $B\, S^{-1} B = -S$, (6) ${}^t d\rho(T)\, S + S\, d\rho(T) = 0$ for all $T \in \mathfrak{k}$, (7) $d\rho(Z)\, S - S\, d\rho(Z) = 0$ for all $Z \in \mathfrak{p}$; where $\mathfrak{g}$ = the Lie algebra of G, $\mathfrak{k}$ = the Lie algebra of K, $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ is the Cartan decomposition. The condition (6) implies that ρ sends K into the maximal compact subgroup $Sp(B) \cap O(S) = \{ m \in Sp(B) ;\ {}^t m\, S\, m = S \}$ of $Sp(B)$. So the representation ρ induces a mapping

τ of $X = G/K$ into $Sp(B) / Sp(B) \cap O(S)$; the latter is a symmetric domain holomorphically isomorphic to the Siegel upper half space $H^{(N/2)}$. This mapping τ is called an Eichler mapping. Satake determined all the representations which induce holomorphic Eichler mappings.

Let us fix such B and S. For a point x of X, put $J(x) = \rho(g)S^{-1} B \rho(g)^{-1}$, where $x = \nu(g)$, $g \in G$. We see easily that: (8) $J(x)$ is a well-defined matrix valued function on X; (9) $J(\gamma x) = \rho(\gamma) J(x) \rho(\gamma)^{-1}$ for $\gamma \in \Gamma$; (10) $J(x)^2 = -1$. Hence, for a fixed x, $J(x)$ defines a complex structure on $R^N/Z^N = F$. Moreover this complex torus $(F, J(x))$ is an abelian variety. By assigning the complex structure $J(x)$ to every fibre $x \times F$ of the product $X \times F$, we get a family of abelian varieties $\{ (F, J(x)) \mid x \in X \}$. The natural mapping $\tilde{p}: X \times F \longrightarrow V$ transfers the complex structure $J(x)$ of $x \times F$ to a complex structure J_Q of a fibre $F_Q = \pi^{-1}(Q)$ of V, where $p(x) = Q$. The equation (9) shows that this induced complex structure of F_Q is independent of the choice of the point x such that $p(x) = Q$. Therefore each fibre F_Q of V has a structure of abelian variety. Furthermore if the Eichler mapping τ is holomorphic, then we can show that the total space V has a good complex structure J compatible with every J_Q and with the complex structure of U, and that V is a projective algebraic variety.

This result combined with Satake's list of holomorphic Eichler mappings gives us a rough classification of family of abelian varieties of our type. One important consequence is the existence of such a family over a symmetric domain attached to an orthogonal group.

§2. The fibre variety $W_N^{(h)}$ defined in §9 of Shimura's talk "The zeta-function of an algebraic variety..." (quoted hereafter as [ZF]) is an example of our V. In this case $G = SL_2(R)$, $X =$ the upper half plane, $\Gamma = \Gamma_N(\mathfrak{O})$ (cf. [ZF, §6]). Here I'd like to discuss some corollaries of the formula given in the last page of [ZF].

Let $\mathfrak{K}$ be a field of algebraic functions of one variable, over a finite field κ, and let $\mathfrak{K}'$ be an unramified Galois extension of $\mathfrak{K}$. Denote by $\mathfrak{G}$ the Galois group. Let R be a representation of $\mathfrak{G}$ by $N \times N$ matrices with entries in a field P. For a prime divisor $\mathfrak{p}$ of $\mathfrak{K}/\kappa$, let $f_{\mathfrak{p}}$ denote the degree of $\mathfrak{p}$ over κ. Take an extension $\mathfrak{P}$ of $\mathfrak{p}$ to $\mathfrak{K}'$. Denote by $\sigma_{\mathfrak{P}}$ the Frobenius automorphism of $\mathfrak{P}$. Then the polynomial $\det(1 - R(\sigma_{\mathfrak{P}}) u^{f_{\mathfrak{p}}})$ is independent of the extension $\mathfrak{P}$; it depends only on $\mathfrak{p}$. Now put

$$L(\mathfrak{K}'/\mathfrak{K},\ R,\ u) = \prod \det(1 - R(\sigma_{\mathfrak{p}})u^{f_{\mathfrak{p}}})^{-1}.$$

This is a formal power series in the variable u with coefficients in P.

The fibre variety $W_N^{(1)} \xrightarrow{\pi} V_N$ has a model which is defined over Q; and for almost all p, the reduction $\widetilde{W}_N^{p(1)}$ of $W_N^{(1)}$ modulo $\mathfrak{p}$ has also a structure of fibre variety over $\widetilde{V}_N^{p}$, whose fibres are abelian varieties $\widetilde{A}_x$ of dimension 2. Take a generic point x of $\widetilde{V}_N^{p}$ over the prime field κ, and consider the fibre $\widetilde{A}_x$ of $\widetilde{W}_N^{p(1)}$ at x. For a prime number $\ell \nmid p$, the coordinates of ℓ^{ν}-th division points of $\widetilde{A}_x$ generate a Galois extension $\mathfrak{K}(\widetilde{A}_x, \ell^{\nu})$ over $\mathfrak{K} = \kappa(x)$. The Galois group $\mathfrak{g}$ of $\mathfrak{K}' = \bigcup_{\nu=1}^{\infty} \mathfrak{K}(A_x, \ell^{\nu})$ over $\mathfrak{K}$ has an ℓ-adic representation M_ℓ^* of size 4. Moreover, in this case, M_ℓ^* is equivalent to a direct sum $\begin{pmatrix} \mu_\ell^* & 0 \\ 0 & \mu_\ell^* \end{pmatrix}$ where μ_ℓ^* is a representation of $\mathfrak{g}$ by 2×2 ℓ-adic matrices. Take a symmetric tensor representation $\underbrace{\square\square\square\square\square\square}_{n}$ of degree n of $GL(2, Q_\ell)$. Then, we have,

$$(1) \qquad L(\mathfrak{K}'/\mathfrak{K}, \underbrace{\square\square\square\square}_{n} \circ \mu_\ell^*,\ u) = \begin{cases} H^N_{n+2}(p, u) & (n > 0), \\ H^N_2(p, u) \,/\, (1-u)(1-pu) & (n = 0), \end{cases}$$

where $H^N_m(p, u) = \det(\ 1 - T^N_m(p)\,u + p\ T^N_m(p,p)\,u^2\ )$ (cf. [ZF]).

From this equality (1) we can deduce the following results. The normal subgroup $\Gamma_{N\ell}(\mathfrak{O})$ of $\Gamma_N(\mathfrak{O})$ defines a covering Riemann surface $\Gamma_{N\ell}(\mathfrak{O}) \backslash X$ of $\Gamma_N(\mathfrak{O}) \backslash X$. This algebraic curve $\Gamma_{N\ell}(\mathfrak{O}) \backslash X$ has also a model defined over Q. Consider the Jacobian variety $J(\mathfrak{O}, N\ell)$ of it, defined over Q, and consider the algebraic number field $Q(\ J(\mathfrak{O}, N\ell),\ \ell\ )$ generated over Q by all the coordinates of all the ℓ-th division points of $J(\mathfrak{O}, N\ell)$. This is a Galois extension over Q. For a rational prime p, denote by f_p the degree of a prime divisor $\mathfrak{p}$ of p in $Q(J(\mathfrak{O}, N\ell), \ell)$. Then, for almost all primes p such that $p \equiv 1 \mod \ell$,

$$(2) \qquad f_p = \text{some power of } \ell\ (= 1 \text{ or } \ell, \text{ or } \ell^2 \ldots)$$

$$\Longleftrightarrow \begin{cases} H^N_{n+2}(p, u) \equiv (1-u)^{2d_{n+2}} \mod \ell, \\ \text{for } n = 0, 2, 4, \ldots, \ell-1, \quad \text{where} \end{cases}$$

d_m = the dimension of the space of holomorphic $\Gamma(\mathfrak{O}, N)$ - automorphic forms of weight m .

Our method cannot be applied for $\Gamma = SL(2, Z)$, because we assumed that $\Gamma \backslash X$ is compact. But we may conjecture that the same result (2) holds also for $SL(2, Z)$. If we assume this, we can deduce the following relations for the Ramanujān's function $\tau(p)$, where $x \prod_{n=1}^{\infty} (1 - x^n)^{24} = \sum_{n=1}^{\infty} \tau(n)\, x^n$.

(!) $p \equiv 1 \ (3)$ implies $\tau(p) \equiv 2 \ (3)$,

(!!) $p \equiv 1 \ (5)$ implies $\tau(p) \equiv 2 \ (5)$,

(!!!) $p \equiv 1 \ (7)$ implies $\tau(p) \equiv 2 \ (7)$,

(?) $p \equiv 1 \ (23)$, and p is a product of two principal ideals in $Q(\sqrt{-23})$, then $\tau(p) \equiv 2 \ (23)$.

(??) The set $\{ p \text{ rational prime number} \mid p \equiv 1 \ (\ell),\ \tau(p) \equiv a \ (\ell) \}$ has a definite Tschebotarev's density.

The first 3 of these relations are classical. The classical congruence relation $1 - \tau(p) + p^{11} \equiv 0 \ (691)$ cannot be obtained in this way.

PART II

by

Goro Shimura

§1. Field of moduli of a polarized abelian variety.

We always take C as the universal domain. Let S be an algebra over Q with identity element. We consider a structure $\mathcal{P} = (A, \mathcal{C}, \Theta)$ formed by an abelian variety A, a polarization $\mathcal{C}$ of A, and an isomorphism Θ of S into $\mathrm{End}_Q(A)$. For a finite set $\{t_1, \ldots, t_r\}$ of points on A, we consider a structure $\mathcal{Q} = \mathcal{P}(t_1, \ldots, t_r) = (A, \mathcal{C}, \Theta; t_1, \ldots, t_r)$. Let $\mathcal{Q}' = (A', \mathcal{C}', \Theta'; t_1', \ldots, t_r')$ be another structure with the same S. We say that $\mathcal{Q}$ and $\mathcal{Q}'$ are isomorphic if there exists an isomorphism λ of A to A' which sends $\mathcal{C}$ to $\mathcal{C}'$ and such that $\lambda\,\Theta(a) = \Theta'(a)\,\lambda$ $(a \in S)$, $\lambda t_i = t_i'$ $(i = 1, \ldots, r)$. $\mathcal{Q}$ is said to be defined over a field k if A is defined over k as abelian variety, $\mathcal{C}$ contains a divisor rational over k, the elements of $\Theta(S) \cap \mathrm{End}(A)$ are defined over k, and the t_i are rational over k. If k is such a field and σ is an isomorphism of k to another field k', then we get naturally a structure $\mathcal{Q}^\sigma = (A^\sigma, \mathcal{C}^\sigma, \Theta^\sigma; t_1^\sigma, \ldots, t_r^\sigma)$. One can prove that there exists a subfield k_0 of C with the following property:

(1.1) <u>Let σ be an automorphism of C. Then $\mathcal{Q}$ and $\mathcal{Q}^\sigma$ are isomorphic if and only if σ is the identity mapping on k_0.</u>

Such a k_0 is uniquely determined by $\mathcal{Q}$ and is called <u>the field of moduli of</u> $\mathcal{Q}$.

§2. Analytic families of polarized abelian varieties.

According to Albert, all the division algebras over Q with positive involutions are classified into the following four types:

(Type I)	a totally real algebraic number field F.
(Type II)	a totally indefinite quaternion algebra over F.
(Type III)	a totally definite quaternion algebra over F.
(Type IV)	a division algebra with an involution of the 2nd kind over F, whose center is a totally imaginary quadratic extension of F.

Let S be an algebra belonging to these types and let μ be a positive involution of S. Let Φ be a representation of S by complex matrices of size n.

Then $\mathcal{P} = (A, \mathcal{C}, \theta,)$ is said to be of type (S, Φ, μ) if: (i) $\dim(A) = n$; (ii) the representation of $\theta(a)$ $(a \in S)$ by a complex coordinate system of A is equivalent to Φ; (iii) the involution of $\mathrm{End}_Q(A)$ determined by $\mathcal{C}$ coincides with $\theta(a) \longrightarrow \theta(a^\mu)$ on $\theta(S)$. Such a $\mathcal{P}$ does not exist unless the following condition is satisfied:

(2.1) <u>The direct sum of Φ and its complex conjugate $\overline{\Phi}$ is equivalent to a rational representation of</u> S.

Let $\mathcal{P} = (A, \mathcal{C}, \theta)$ be of type (S, Φ, μ), and let C^n/D be a complex torus isomorphic to A. We see that $Q \cdot D$ has naturally a structure of a left S-module of rank m where $m = 2n/[S : Q]$. Put $W = S^m$ and take an S-isomorphism f of W to $Q \cdot D$. Put $L = f^{-1}(D)$. Let Y be the basic polar divisor in $\mathcal{C}$, and let $E(x, y)$ be the Riemann form determined by Y. Then there exists an anti-hermitian form $T(x, y)$ on W such that $E(f(x), f(y)) = \mathrm{tr}_{S/Q}(T(x, y))$. The structure (W, T, L) is uniquely determined by $\mathcal{P}$ up to isomorphisms. We say that $\mathcal{P}$ is of type $(S, \Phi, \mu; T, L)$. If S is of (Type I, II, III), T can be arbitrary. Suppose that S belongs to (Type IV). Put $g = [F : Q]$. Let $\tau_1, \ldots, \tau_g$ be inequivalent absolutely irreducible representations of S whose restrictions to F are distinct. Let r_ν be the multiplicity of in Φ. Then T must satisfy:

(2.2) <u>For each ν, the complex hermitian matrix $\sqrt{-1}$ (T) has exactly r_ν negative characteristic roots.</u>

Let $u_1, \ldots, u_r \in W$. We say that $\mathcal{Q} = \mathcal{P}(t_1, \ldots, t_r)$ is of type $(S, \Phi, \mu; T, L; \{u_i\})$ if $t_i = f(u_i) \bmod D$ for the above f.

Put $M = L + \sum_{i=1}^{r} Z u_i$, and

$$\begin{aligned} G(T) &= \{ B \in \mathrm{End}_S(W) \mid T(xB, yB) = T(x, y) \}, \\ \Gamma(T, L) &= \{ B \in G(T) \mid LB = L \}, \\ \Gamma(T, M/L) &= \{ B \in \Gamma(T, L) \mid M(1 - B) \subset L \}, \\ X &= G(T)_R / \text{ (maximal compact subgroup)}. \end{aligned}$$

Then X is a bounded symmetric domain, and $\Gamma(T, M/L)$ is a properly discontinuous group operating on X.

<u>Theorem 1.</u> <u>If Φ satisfies (2.1) and T satisfies (2.2), then for a given $(S, \Phi, \mu; T, L; \{u_i\})$, there exists an analytic family $\sum = \{\mathcal{Q}_z \mid z \in X\}$ with the following properties:</u>

(1) Every member $\mathcal{Q}_z$ is of type $(S, \Phi, \mu; T, L; \{u_i\})$.

(2) Every $\mathcal{Q}$ of type $(S, \Phi, u; T, L; U_i)$ is isomorphic to a member of Σ.

(3) $\mathcal{Q}_z$ and $\mathcal{Q}_w$ are isomorphic if and only if there exists an element B of $\Gamma(T, M/L)$ such that $B(z) = w$.

Theorem 2. There exist meromorphic functions $f_1, \ldots, f_\lambda$, $g_1, \ldots, g_\kappa$ on X with the following properties:

(1) $C(f_1, \ldots, f_\lambda)$ is the field of all automorphic functions on X with respect to $\Gamma(T, M/L)$.

(2) $Q(f_1(z), \ldots, f_\lambda(z))$ is the field of moduli of $\mathcal{Q}_z$ if all the f_i and g_j are holomorphic at z.

(3) If k is the algebraic closure of Q in $Q(f_1, \ldots, f_\lambda)$, then $k(f_1, \ldots, f_\lambda)$ and C are linearly disjoint over k.

§3. Field of definition for X/Γ and fibre varieties of Kuga's type.

Assume that the following conditions are satisfied:

(3.1) For a generic member $\mathcal{Q}_z = (A_z, \mathcal{C}_z, \Theta_z; ..)$ of Σ, one has $\Theta_z(S) = \mathrm{End}_Q(A_z)$.

(3.2) $\Gamma(T, M/L)$ has no element of finite order other than the identity element.

(3.3) $X/\Gamma(T, M/L)$ is compact.

Let ρ be a representation of $G(T)_R$ into $GL(W_R)$. Then all the assumptions in §1 of Part I are satisfied by this ρ; for reader's convenience, we give a list of corresponding symbols:

Part I:	G	X	ρ	R^n	Z^n	B	Γ
Part II:	$G(T)_R$	X	ρ	W_R	L	$tr(T)$	$\Gamma(T, M/Z)$

Let $U = X/\Gamma(T, M/L)$ and let V be the fibre variety constructed in Part I out of these data, of which the base is U and each fibre is the product of h copies of A_z, where h is a fixed positive integer. Let π be the natural projection of V to U. (The above list is for the case $h = 1$.)

Theorem 3. Let k be as in (3) of Th. 2. Suppose that (3.1), (3.2) and (3.3) are satisfied. Then there exist projective non-singular models for U, V, π, which are defined over k.

§4. The field k as a class-field.

Let k be the algebraic number field determined by (3) of Th. 2.

Theorem 4. Let S be of (Type I, II.) Let $\mathfrak{O}$ be a maximal order in S, and $\mathfrak{a}$ an integral two-sided $\mathfrak{O}$-ideal. Suppose that $\mathfrak{O}L \subset L$ and $M = \mathfrak{a}^{-1}L$. Let a be a positive integer such that $\mathfrak{a} \cap Z = aZ$. Then $k = Q(e^{2\pi i/a})$.

For the algebra of (Type III), one may conjecture that k is a cyclotomic field.

Theorem 5. Let S be an imaginary quadratic extension of a totally real algebraic number field F. Put $S^* = Q(\mathrm{tr}(\Phi(x)) \mid x \in S)$. Let $\mathfrak{O}$ be the ring of integers in S, and $\mathfrak{a}$ an integral ideal in F. Suppose that $\mathfrak{O}L \subset L$, $M = \mathfrak{a}^{-1}L$. Then, for suitabley chosen T and L, the field k can be determined as follows:

(Case 1) If Φ is equivalent to $\bar{\Phi}$, then $S^* = Q$, and $k = Q(e^{2\pi i/a})$, where a is the positive integer such that $\mathfrak{a} \cap Z = aZ$.

(Case 2) If Φ is not equivalent to $\bar{\Phi}$, then S^* is a totally imaginary quadratic extension of a totally real algebraic number field F^*, and k is the class-field over S^* corresponding to the following ideal group H in S^*:

$$H = \left\{ \mathfrak{c} \;\middle|\; \prod_{\lambda=1}^{h} \left(\frac{\mathfrak{c}^{\sigma_\lambda}}{\mathfrak{c}^{\sigma_\lambda \rho}}\right)^{\nu_\lambda} = (y),\ y\bar{y} = 1,\ N(\mathfrak{c}) \equiv y \equiv 1 \mod^* \mathfrak{a} \text{ for an element } y \text{ of } S \right\}, \text{ if } m \text{ is even;}$$

$$H = \left\{ \mathfrak{c} \;\middle|\; \prod_{\lambda=1}^{h} \mathfrak{c}^{\sigma_\lambda} \cdot \left(\frac{\mathfrak{c}^{\sigma_\lambda}}{\mathfrak{c}^{\sigma_\lambda \rho}}\right)^{\nu_\lambda} = (y),\ y\bar{y} = N(\mathfrak{c}),\ y \equiv 1 \mod^* \mathfrak{a} \text{ for an element } y \text{ of } S \right\}, \text{ if } m \text{ is odd.}$$

Here $\sigma_1, \ldots, \sigma_h$ are isomorphisms of S^* into C whose restrictions to F^* are distinct; the ν_λ are certain integers determined by S and Φ; mod* means the multiplicative congruence.

We can actually determine k for any T and L; however, the expression for corresponding H is rather complicated in the general case.

§5. Bottom fields.

Let U be a projective variety. Suppose that there exists a subfield B of C with the following property:

(5.1) Let σ be an automorphism of C. Then U is birationally equivalent to U^σ if and only if σ is the identity mapping on B.

Such a field B is uniquely determined by U, if it exists. We call B the bottom field for U. If U is defined over an algebraic number field, then the bottom field for U exists. If U is a curve, the bottom field for U exists and coincides with the field of moduli of the canonically polarized jacobian variety of U.

Let F be a totally real algebraic number field of degree g, and D a quaternion algebra over F. Then we may identify $D \otimes_Q R$ with $M_2(R) \times \ldots \times M_2(R) \times K \times \ldots \times K$, where K is the division ring of real quaternions. Let t be the number of copies of $M_2(R)$. We assume that $0 < t < g$. Let $\mathfrak{O}$ be a maximal order in D and $\mathfrak{a}$ an integral ideal in F. Put

$$\Gamma(\mathfrak{O};\mathfrak{a}) = \left\{ x \in \mathfrak{O} \;\middle|\; xx^{\iota} = 1,\ x \equiv 1 \mod \mathfrak{a}\mathfrak{O} \right\},$$

where ι is the canonical involution of D. Projecting $\Gamma(\mathfrak{O};\mathfrak{a})$ to the partial product $M_2(R)^t$, we may consider it as a discontinuous group operating on $X^t = \left\{ (z_1, \ldots, z_t) \in C^t \;\middle|\; \mathrm{Im}(z_1) > 0, \ldots, \mathrm{Im}(z_t) > 0 \right\}$.

Let $p_{\infty 1}, \ldots, p_{\infty t}$ be the infinite prime spots of F where D is unramified, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the prime ideals of F where D is ramified. Let $I(D/F)$ be the subgroup of the ideal-group of F, generated by the following three kinds of ideals: (1) the principal ideals (a) such that a is totally positive; (ii) the squares of all ideals in F; (iii) the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$.

Let F^* be the field generated over Q by the elements $\sum_{i=1}^{t} x^{\sigma_i}$ for all $x \in F$, where $\sigma_1, \ldots, \sigma_t$ are the isomorphisms of F into R corresponding to $p_{\infty 1}, \ldots, p_{\infty t}$.

Theorem 6. Suppose that: (i) there is no automorphism of F, other than the identity mapping, which leaves invariant $\{p_{\infty 1}, \ldots, p_{\infty t}; \mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ as a whole; (ii) for every maximal order $\mathfrak{O}$, the group $\Gamma(\mathfrak{O};\mathfrak{a})$ has no element of finite order other then ± 1. Then the composite of F^* and the bottom field for $X^t/\Gamma(\mathfrak{O};\mathfrak{a})$ is the class-field over F^* corresponding to the ideal-group

$$\left\{ \mathfrak{c} \;\middle|\; \prod_{i=1}^{u} \mathfrak{c}^{\tau_i} \in I(D/F) \right\},$$

where $\tau_1, \ldots, \tau_u$ are certain isomorphisms of F^* into R, determined by F and $\sigma_1, \ldots, \sigma_t$.

REPORT ON THE COMMUTATIVE ALGEBRA SEMINAR

by

Pierre Samuel

An informal Seminar on Commutative Algebra met on Tuesdays and Thursdays at 1:30 P.M. There were talks by P. Samuel (Paris), M. Auslander (Brandeis), S. Lichtenbaum (Harvard), H. Schlessinger (Harvard), Dock Sang Rim (Brandeis) and N. Greenleaf (Harvard). We are going to give a summary of these talks.

§ 1. Flat Modules (P. Samuel)

Very recently a young French mathematician, Daniel Lazard, has proved the following theorem:

Theorem - Let A be any ring (commutative or not) and M a flat A-module. Then M is a direct limit of free A-modules of finite rank (with respect to a filtering ordered set of indices).

The converse ("every direct limit of free modules is flat") is well known. The theorem was known to H. Bass in the case of a local ring A. A Russian published in the Doklady a proof that contained mistakes, but these mistakes can be corrected. Lazard's proof (published in a Comptes Rendus note in June or July, 1964) is independent and runs as follows:

Lemma - Let P be a finitely presented A-module, M a flat A-module, and $u: P \longrightarrow M$ a homomorphism. Then there exists a free module F of finite rank and homomorphisms $P \xrightarrow{v} F \xrightarrow{w} M$ such that $u = w \circ v$.

Proof: We have an exact sequence $F_1 \xrightarrow{a} F_0 \xrightarrow{b} P \longrightarrow 0$ with F_1, F_0 free of finite rank; set $c = u \circ b \in \mathrm{Hom}(F_0, M) = F_0^* \otimes M$ let F^1 be a free module such that $F' \longrightarrow F_0^* \xrightarrow{{}^t a} F_1^*$ is exact. Then $F' \otimes M \xrightarrow{\phi} F_0^* \otimes M$ is exact since M is flat. Since $c \circ a = 0$, c is the image by ϕ of an element d of $F' \otimes M$; there exists a free submodule F'' of finite rank of F' such that $d \in F'' \otimes M$. Set $F = (F'')^*$, so that $F'' = F^*$; then d may be viewed as an element of $F^* \otimes M = \mathrm{Hom}(F, M)$, and is the w were looking for. The transpose e of $F^* \longrightarrow F_0^*$ is a homomorphism of F_0 into F such that $e \circ a = 0$, thus gives $v: P \longrightarrow F$. Q.E.D.

Remark: The lemma proves immediately that a finitely presented flat module P is projective: take $M = P$, $u =$ identity.

One then represents the given flat module M as the direct limit of a large direct system $(P_\alpha, \phi_{\alpha\beta})$ of finitely presented modules: writing $0 \longrightarrow R \longrightarrow A^{(M \times \mathbb{Z})} \longrightarrow M \longrightarrow 0$, the indices α are pairs (I, S) where I is a finite subset of $M \times \mathbb{Z}$ and S a finitely generated submodule of $A^I \cap R$, P_α is A^I/S, $P_\alpha \longrightarrow M$ the obvious map, and the order relation $(I,S) \leq (I',S')$ means $I \subset I'$ and $S \subset S'$. For each α, $P_\alpha \longrightarrow M$ factors through a free module F_α of finite rank: $P_\alpha \longrightarrow F_\alpha \longrightarrow M$ (by the lemma). Now, the direct system $(P_\alpha ; \phi_{\alpha\beta})$ being large enough, there exists $\beta \geq \alpha$ such that $P_\alpha \xrightarrow{\phi_{\beta\alpha}} P_\beta \longrightarrow M$ is isomorphic to $P_\alpha \longrightarrow F_\alpha \longrightarrow M$. In other words the free P_α's are cofinal in the system, and M is their limit. This proves Lazard's theorem.

Many applications can be given. For example, if M is a flat module over a commutative ring A, then the tensor algebra $T(M)$, the exterior algebra $\wedge(M)$ and the symmetric algebra $S(M)$ are flat A-modules. In particular, if A is an integra domain, $S(M)$ is torsion-free, whence is also an integral domain(setting T = set of non zero elements of A, $S_A(M) \longrightarrow T^{-1} S_A(M)$ is injective, and we have $T^{-1}S_A(M) = S_{T^{-1}A}(T^{-1}M)$ = polynomial ring over the quotient field $T^{-1}A$ of A = integral domain).

§2. Reflexive modules and factorial rings. (P. Samuel)

The proofs may be found in P. Samuel, "Modules réflexifs et anneaux factoriels", Bull. Soc. Math. France, 1964 (see also Seminaire Dubreil, 1963-64).

Here A denotes a local noetherian Macaulay ring. For an A-module M, $d\rho(M)$ (or $d\rho_A(M)$) denotes the "depth" of M, i.e., the number of elements of a maximal M-sequence. Let q be an integer ≥ 0. Then the following two statements are equivalent:

(P_q) Every A-sequence with $q' \leq q$ elements is an M-sequence.

(P'_q) For every $p \in$ Spec (A), we have $d\rho A_p(M_p) \geq \inf(q, d\rho A_p(A_p)) = \inf(q, h(p))$

If M has finite homological dimension, these statements are equivalent to:

(P''_q) For every $P \in$ Spec(A), we have $hd_{A_p}(M_p) \leq \sup(0, h(p) - q)$

M. Auslander noticed that (P_q) is implied by:

(P'''_q) There exists an exact sequence $0 \longrightarrow M \longrightarrow F_1 \longrightarrow F_2 \longrightarrow \text{---} \longrightarrow F_q$ where the F_i's are free modules of finite rank.

According to H. Bass, the converse $(P_q) \Longrightarrow (P'''_q)$ is true if A is a Gorenstein ring, not otherwise.

If A is a domain, (P_1) means that M is torsion-free. If A is an integrally closed domain, (P_2) means that M is reflexive (i.e., that $M \longrightarrow M^{**}$ is bijective, or, equivalent by, that M is torsion-free and that $M = \bigcap_{h(p) = 1} M_p)$. If A is regular, $(P_{\dim(A)})$ means that M is free. Thus the module-properties (P_q) seem to correspond to ring-properties. This is corroborated by the following facts, about the symmetric algebra $S(M) = \bigoplus_{n \geq 0} S^n(M)$ of a module M over A :

1) $S(M)$ <u>is a domain iff</u> A <u>is a domain and each</u> $S^n(M)$ <u>is torsion free over</u> A (i.e., <u>has property</u> (P_1)).
2) $S(M)$ <u>is factorial iff</u> A <u>is factorial and each</u> $S^n(M)$ <u>is reflexive over</u> A (i.e., <u>has property</u> (P_2)).
3) $S(M)$ <u>is regular iff</u> A <u>is regular and each</u> $S^n(M)$ <u>is a projective</u> A-<u>module</u> (i.e., has property $(P_{\dim(A)})$ if A is local) (notice that, if M is projective, each $S^n(M)$ is also projective).

Finally we give some examples in the case of a module M of <u>homological dimension one</u>, i.e., defined by n generators x_i and $s \leq n$ linearly independent relations $\sum_{c=1}^{n} a_{ji} x_i = 0$. Let $\mathfrak{a}$ be the ideal generated by the $s \times s$ minors of the matrix (a_{ij}).

a) M has property (P_q) iff $\mathfrak{a}$ is not contained in any prime ideal of height q of A .

b) If $s = 1$ (only one relation) and if M has property (P_q), then all the symmetric powers $S^k(M)$ $(k \geq 0)$ have property (P_q). Thus, if A is factorial, $A\left[X_1, \ldots, X_n\right] / (\sum_{c=1}^{n} a_i x_i)$ is factorial iff the ideal $\sum_{i=1}^{n} A\, a_i$ is not contained in any prime ideal of height 2.

c) In general the symmetric powers of a reflexive module are not reflexive. Take for A a regular local ring of dimension 3. Let $(a, b, c,)$ be a system of generators of its maximal ideal. Consider the linearly independen vectors $u = (a, b, 0, c, 0)$, $v = (0, a, b, 0, c)$ in A^5. The module $M = A^5 / (Au + Av)$ is reflexive by a). However $S^2(M)$ has homological dimension 2, whence is not reflexive (by (P''_q)).

3. <u>Power series over integrally closed domains.</u> (P. Samuel).

It is well known and easy to prove that, if A is <u>completely</u> integrally closed domain (e.g. a noetherian integrally closed domain), then $A\left[X\right]$ and $A\left[\left[X\right]\right]$ also are. On the other hand, if A is an integrally closed domain, so is the polynomial ring $A\left[X\right]$ (this is not so easy to prove). However there exist integrally closed domains A such that the power series ring $A\left[\left[X\right]\right]$ is not integrally closed.

In fact take for A an integrally closed domain in which there exist a non-unit a and a non-zero element b such that $b \in \bigcap_{n=1}^{\infty} Aa^n$ (e.g. a valuation ring of height ≥ 2). One constructs by induction on the coefficients a power series $u(x) = u_0 + u_1 x + \ldots + u_n x^n + \ldots$ such tha

$$(Xu(X))^2 + a\,Xu(X) + X = 0$$

($au_0+1 = 0$, $u_0^2+au_1 = 0$, $2u_0u_1+au_2 = 0$, etc.) . We have $a^{2m+1}u_n \in A$. The series $Xu(X)$ is integral over $A[[X]]$, belongs to its quotient field (since $bXu(X) \in A[[X]]$, and is not in $A[[X]]$ (since $u_0 = \frac{1}{a}$)

A. Seidenberg pointed out the following somewhat simpler example (in which A is as above, and is supposed to contain Q): the series $\sqrt{a^2+x} = a\sqrt{1+\frac{x}{a}} = a\left(1+\frac{x}{2a} - \frac{1}{8}\frac{x^2}{a^2} + \frac{1}{16}\frac{x^3}{a^3} \cdots\cdots\right)$

§ 4. Modules over unramified regular local rings. (M. Auslander)

Let R be an unramified (e.g. equicharacteristic) regular local ring, and A,B two finitely generated R-modules. M. Auslander proved:

<u>Theorem</u> - <u>If</u> $\mathrm{Tor}_i(A,B) = 0$, <u>then</u> $\mathrm{Tor}_j(A, B) = 0$ <u>for any</u> $j \geq i$.

One conjectures that the theorem is true for any local ring R , provided the modules A and B have finite homological dimensions. We are going to give various applications of this theorem. Henceforth R denotes an unramified regular local ring, and all modules are finitely generated.

a) Suppose that $A \otimes B$ is $\neq 0$ (i.e. $A \neq 0$ and $B \neq 0$) and is torsion free; then A and B are torsion-free, we have $\mathrm{Tor}_i(A, B) = 0$ for any $i > 0$, and $hd(A) + hd(B) < \dim R$. Consequently, if the n-fold tensor product $A \otimes \cdots \otimes A$ ($n = \dim R$) is torsion-free, then A is free. Also, if $A^* \neq 0$, and if either $A \otimes A \otimes A^*$ or $A \otimes A^* \otimes A^*$ is torsion free, then A is free. Notice that A is free iff $A \otimes A^*$ is reflexive.

b) If $hdA = hdA^*$, if $A \otimes A^*$ is torsion-free, and if A_p is free for every prime ideal $p \neq m$ (m: maximal ideal of R), then A is free or has homological dimension $\frac{n-1}{2}$ (if $n = \dim R$ is odd). For n odd, the "kernel-image" in the middle term of a free resolution of A/m has the above properties. These "middle modules" have probably many other properties.

c) Consider a free (or flat) complex $\cdots \longrightarrow X_i \longrightarrow X_{i+d} \longrightarrow X_{i+2d} \longrightarrow \cdots$, a module C , and the "universal-coefficient-map":

$$\phi : H_q(X) \otimes C \longrightarrow H_q(X \otimes C)$$

If Z_q denotes the cokernel of $X_q \longrightarrow X_{q+d}$, the cokernel of ϕ is $\mathrm{Tor}_1(Z_q, C)$ and its kernel is $\mathrm{Tor}_2(Z_q, C)$. The theorem shows that, if ϕ is onto, then it is an isomorphism. For example, if $M^* \otimes A \longrightarrow \mathrm{Hom}(M,A)$ is onto, then it is an isomorphism. One gets also relations between Ext and Tor, and examples of modules M for which every M-sequence is an R-sequence.

d) Given two R-modules A, A^1, we write $[A] = [A^1]$ (resp. $[A] \leq [A^1]$) if $hd_{r_p}(A_p) =$ (resp. $\leq$) $hd_{r_p}(A^1_p)$ for every prime ideal p of A. One shows that Supp $(\mathrm{Tor}_i(A,B))$ is the set of all $\alpha \in \mathrm{Spec}(A)$ for which there exists $p \in \mathrm{Spec}(A)$, $p \subset \alpha$ such that $hd_{R_p}(A_p) + hd_{R_p}(B_p) \geq \dim(R_p) + i$. The relations between Ext and Tor quoted in c) show that, if $A \neq 0$ and $\mathrm{Ext}^{r}(M,A) = 0$, then $\mathrm{Ext}^{r}(M,B) = 0$ for $[B] \leq [A]$; in particular $\mathrm{Ext}^{r}(M,R) = 0$. As a consequence, $\mathrm{Ext}^q(A,A) = 0$ iff $hd(A) < q$, and $\mathrm{Ext}^1(A,A) = 0$ iff A is free:

(More details may be found in M. Auslander, Illinois Journal, and Proc. Int. Congress of Stockholm).

§ 5. Modules of differentials: (S. Lichtenbaum and M. Schlessinger)

Given two commutative rings A, B and a ring homomorphism $A \longrightarrow B$, we denote by $\Omega_{B/A}$ the B-module of A-differentials of B; let us recall that it is a B-module, together with an A-derivation $d : B \longrightarrow \Omega_{B/A}$, which are "universal" for the A-derivations of B into B-modules. Its elements are sometimes called the "Kähler differentials" of B Modules of differentials have also been studied recently by Nakai, Suzuki, Berger, Kunz and Jouanolou.

If $A \longrightarrow B \longrightarrow C$ is a diagram in the category of rings, then we have the well known exact sequence

(1) $$C \otimes_B \Omega_{B/A} \longrightarrow \Omega_{C/A} \longrightarrow \Omega_{C/B} \longrightarrow 0$$

Let M be a C-module. Then $(1_1) = (1) \otimes M$ and $(1') = \mathrm{Hom}((1),M)$ are exact sequences We are going to define functors $T_i(B/A, M)$ and $T^i(B/A, M)$ $(i = 0, 1, 2)$ which permit to extend (1') and (1") to exact sequences with nine terms. If $C = B/I$, it is easily seen that I/I^2 may be added at the left of (1). In Grothendieck-Dieudonnè EGA IV, (1) is extended to a six-terms exact sequence.

a) Definition of the functors (for $A \longrightarrow B$)

Let P be a polynomial ring over A and I an ideal in P such that $0 \longrightarrow I \longrightarrow P \longrightarrow B \longrightarrow 0$ is exact. Represent I as a factor module of a free P-module F, say $0 \longrightarrow U \longrightarrow F \xrightarrow{e} I \longrightarrow 0$, and define $\phi : F \otimes_P F \longrightarrow F$ by $\phi(x \otimes y) = e(x)y - e(y)x$. Set $U_0 = \mathrm{Im}(\phi)$; we have $IU \subset U_0 \subset IF \cap U$. The "cotangent complex" $L(B/A, P, F)$ is

$$U/U_0 \longrightarrow F \otimes_P B = F/IF \longrightarrow \Omega_{P/A} \otimes B$$

(the last arrow is the composition $F/IF \longrightarrow I/I^2 \xrightarrow{d} \Omega_{P/A} \otimes B$). By the usual technique one proves that, up to homotopies, the complex $L(B/A, P, F)$ is independent of P and F. We denote it by $L(B/A)$ and define $T_i(B/A, M) = H_i(L(B/A) \otimes M)$ and $T^i(B/A, M) = H^i(\mathrm{Hom}_B(L(B/A), M)$ for every B-module M. Classical results show that $T_0(B/A, M = \Omega_{B/A} \otimes M$ and $T^0(B/A, M) = \mathrm{Hom}_B(\Omega_{B/A}, M) = \mathrm{Der}_A(B, M)$.

b) Vanishing properties

We have $T^1(B/A, M) = 0$ for every B-module M iff B is formally smooth over A (i.e. every homomorphism $B \longrightarrow C/J$ where $J^2 = 0$ maybe lifted to $B \longrightarrow C$); this implies $T_1(B/A, M) = 0$ for every M. If A is noetherian and if B is an A-algebra of finite type then the following properties are equivalent: a) $T^1(B/A, M) = 0$ for every M; $T_1(B/A, M) = 0$ for every M; c) B is formally smooth over A; d) B is smooth over A (i.e. B is flat over A and its fibers are absolutely non-singular); e) $\Omega_{B/A}$ is projective and $T_1(B/A, B) = 0$; f) $T^1(B/A, B/m) = 0$ for every maximal ideal m of B; g) $T_1(B/A, B/m) = 0$ for every maximal ideal m of B.

Again, if A is noetherian and if B is an A-algebra of finite type the following are equivalent: a) $T^2(B/A, M) = 0$ for every B-module M; b) $T_2(B/A, M) = 0$ for every B-module M; c) B is locally a complete intersection over A (i.e. if B is represented as a quotient of a polynomial ring P over A by $P \xrightarrow{j} B \longrightarrow 0$, then, for every $p \in \mathrm{Spec}(B)$, B_p is a quotient of $P_{j^{-1}(p)}$ by a regular sequence).

If $K \longrightarrow L$ is a field extension, then $T^2(L/K, M) = T_2(L/K, M) = 0$ for every L-module M; the relations $T^1(L/K, M) = 0$ for all M and $T_1(L/K, M) = 0$ for all M are both equivalent with the separability of L over K. If A and B are domains, $A \subset B$, if B is locally a complete intersection over A , and if the quotient field extension is separable then:

a) $T_1(B/A, B) = 0$ iff $T^1(B/A, M) = \mathrm{Ext}^1_B(\Omega_{B/A}, M)$ for every M ;

b) $T_1(B/A, B)$ is a torsion module iff $T_1(B/A, B) = \mathrm{Ext}^1_B(\Omega_{B/A}, B)$

c) The nine-term exact sequence.

Let $A \longrightarrow B \longrightarrow C$ be a diagram of rings. Given cotangent complexes $L(B/A, P, F)$ and $L(C/B, Q, G)$ there exist a cotangent complex $L(C/A, R, H)$ such that

$$0 \longrightarrow L(B/A, P, F) \otimes C \longrightarrow L(C/A, R, H) \longrightarrow L(C/B, Q, G) \longrightarrow 0$$

is "almost exact". As usual this gives an exact sequence:

$$T_2(B/A, M) \rightarrow T_2(C/A, M) \rightarrow T_2(C/B, M) \rightarrow T_1(B/A, M) \rightarrow T_1(C/A, M) \dashrightarrow T_0(C/B, M) \rightarrow 0$$

where M is any C-module. Similarly for the functors T^i .

As an application, let A be a noetherian local ring, and I, J two ideals of A such that $I \subset J$; set $K = J/I$, $B = A/I$, $C = A/j = B/K$. If j is generated by an A-sequence and K by a B-sequence, then I is generated by an A-sequence. This is proved by writing the exact sequence for $T_i(*, C)$: here the T_0-terms are 0, $T_2(C/B, C) = 0$ by the hypothesis on K , and the T_1-terms give:

$$0 \longrightarrow I/jI \longrightarrow j/j^2 \longrightarrow K/K^2 \longrightarrow 0 \ j$$

by hypothesis j/j^2 and K/K^2 are free C-modules of ranks dim A-dimC and dimB-dim C; whence, by Nakayama, I is generated by dimA-dimB elements, whence by an A-sequence.

§ 6. Cotangent complexes and deformations (S. Lichtenbaum and M. Schlessinger

The notations are as in §5. The construction of cotangent complexes commutes with localization. Hence, given a prescheme X over a prescheme S and a sheaf $\mathcal{F}$ of $\mathcal{O}_X$-modules over X , we get sheaves $T^i(X/S, \mathcal{F})$ (i = 1, 2, 3,); they are coherent if $\mathcal{F}$ is coherent and if the usual finiteness conditions for $X \longrightarrow S$ are satisfied.

a) Ring extensions

Let B be a (commutative) A-algebra and M an A-module; an extension of

B by M is an exact sequence $0 \longrightarrow M \xrightarrow{j} E \longrightarrow B \longrightarrow 0$, where $E \longrightarrow B$ is an algebra-homomorphism and where $j(M)^2 = 0$. The <u>isomorphism classes</u> of such extensions correspond bijectively to the elements of $T^1(B/A, M)$

b) <u>Deformations</u>

Let B be a flat A-algebra ; let us write A as $A = A^1/J$ where j is an ideal of square 0 ($j^2 = 0$) . An <u>infinitesimal deformation</u> of B/A over A^1 is an A^1-flat algebra B^1 such that $B^1/jB1 \simeq B$. Let $\mathrm{Def}(B/A, A^1)$ be the set of isomorphism classes of such deformations. Let $I = j \otimes_A B$ and consider the exact sequence (coming from $A^1 \longrightarrow A \longrightarrow B$)

$$T^1(B/A, I) \longrightarrow T^1(B/A^1, I) \longrightarrow T^1(A/A^1, I) \xrightarrow{\partial} T^2(B/A, I)$$

In $T^1(A/A^1, I) = \mathrm{Hom}_A(I, I)$, we have the identity 1 . Then α) we have $\mathrm{Def}(B/A, A^1) \neq \emptyset$ iff $\partial(1) = 0$ β) If $\partial(1) = 0$, then $\mathrm{Def}(B/A, A^1)$ is a principal homogeneous space over the group $T^1(B/A, I)$

γ) If B is formally smooth over A, $\mathrm{Def}(B/A, A^1)$ has just one element.

Now let X be a scheme over an algebraically closed field k ; we set $T^i = T^i(X/k, \mathcal{O}_X)$. If X is reduced, then $T^1 = \underline{\mathrm{Ext}}^1_{\mathcal{O}_X}(\Omega_X, \mathcal{O}_X)$. Let b be the category of finite dimensional local k-algebras. For $A \in b$, we denote by $F(A)$ the set of isomorphism classes of flat schemes $Y \longrightarrow A$ such that $Y \otimes_A k = X$. Let $k[\varepsilon]$ be the algebra of dual numbers over k ($\varepsilon^2 = 0$). Then we have the exact sequence:

$$0 \longrightarrow A = H^1(X, T^0) \longrightarrow B = F(k[\varepsilon]) \longrightarrow H^0(X, T^1) = b \longrightarrow H^2(X, T^0) - -$$

(Notice that $H^0(X, T^1)$ is the sheaf of germs of deformations). One proves that, if A and B are finite dimensional over k (e.g. if X is proper over k), then there exists a complete local ring R with residue field k and a <u>formal prescheme</u> $\mathfrak{X}$ over R (the "universal deformation" of $X \longrightarrow k$) such that:

(1) $\mathrm{Hom}(R, A) \longrightarrow F(A)$ is surjective for all $A \in b$.

(2) $\mathrm{Hom}(R, k[\varepsilon]) \longrightarrow F(k[\varepsilon])$ is bijective.

If R is chosen minimal, then R and $\mathfrak{X}$ are unique up to a <u>non-canonical</u> isomorphism. The tangent space to R is B .

c) Rigid singularities

Let X be a scheme over an algebraically closed field k , and P an isolated singular point of X . We say that P is *rigid* if $T^1_P = 0$. Then, if $X = \operatorname{Spec} \mathcal{O}_P$, X has only trivial deformations, and the local ring R (see b)) is k .

For example, if X is the cone of $\mathbb{P}_n \times \mathbb{P}_m$ on Segre's imbedding and if P is its vertex, then P is rigid for $n \geq 1$ and $m \geq 2$. This has been proved by Grauert and Kerner (Math. Am.) by analytic methods. An algebraic proof has been given in the lecture, based on the following lemma:

Lemma - If $\mathcal{O}_P$ and T^0_P have depths ≥ 3, then P is rigid.

In fact, from the hypotheses in the lemma one deduces that $T^1_{P_1} = \operatorname{Ext}^1(T^0_P, \mathcal{O}_P)$ has depth ≥ 1 (usual game with resolutions) ; on the other hand T^1_P is a torsion-module since P is an isolated singularity. Hence $T^1_P = 0$ and P is rigid.

This being so, one checks that the vertex P verifies the hypotheses in the lemma.

d) Links with the Kähler different and Riemann-Roch formula.

Let X be a closed subscheme of a projective space $\mathbb{P}$ over a scheme Y , and $z : X \longrightarrow \mathbb{P}$; let I be the sheaf of maximal ideals on X . Suppose that X is locally a complete intersection over Y . Consider the Grothendieck-group of $\mathcal{O}_X$ - modules, and, in this group, the element

$$\mathcal{C}_{X/Y} = \left[z^*\Omega_{P/Y} \right] - \left[I/I^2 \right]$$

This is the class of the Kähler -different of X/Y . With $X \xrightarrow{b} Y \longrightarrow Z$, we have the transitivity formula

$$\mathcal{C}_{X/Y} = f^* (\mathcal{C}_{Y/Z}) + \mathcal{C}(X/Y)$$

The Chern-class $K_{X/Y} = c_1(\mathcal{C}_{X/Y})$ in Pic (X) is interesting; it gives the good canonical class for a curve over a non-perfect field.

The Riemann-Roch formula

$$f_* (\operatorname{ch} x \cdot T(X)) = T(Y) \operatorname{ch} (f_! x)$$

gives here:

$$f_*(T(\mathcal{C}^{-1}_{X/Y})\ \mathrm{ch}\,x) = \mathrm{ch}\,(f_! x)$$

§ 7. Generalized Koszul complexes. (Dock Sang Rim)

This is a report on an article by D. Buchsbaum and Dock Sang Rim (Trans. A.M.S. 1964). Analogous results have been given in an article of Northcott-Eagon.

Let X_{ij} $(1 \leq i \leq m,\ 1 \leq j \leq n,\ m \geq n)$ be independent variables, and I_ρ the ideal generated by the $\rho \times \rho$ -minors of the matrix (X_{ij}) in $\mathbb{Z}\left[(X_{ij})\right] = S.\ (\rho - n)$. The aim is to write a free acyclic resolution of the S-module S/I_ρ. For $n = \rho = 1$ this is done by the classical Koszul complex

$$0 \longrightarrow \bigwedge^m S^m \longrightarrow \ \ldots \longrightarrow \bigwedge^2 S^m \longrightarrow S^m \longrightarrow S \longrightarrow S/(X_1, \ldots, X_m) \longrightarrow 0$$

More generally we have a commutative ring R and a linear map $f\colon R^m \longrightarrow R^n$ $(m \geq n)$, described by a matrix (x_{ij}). We consider $\bigwedge^\rho f\colon \bigwedge^\rho R^m \longrightarrow \bigwedge^\rho R^n$ $(\rho \leq n)$ and have to extend it (on the left) to a free acyclic complex. This is an analogue of the bar-construction. First terms:

$$\ldots \longrightarrow \sum_{s > n-\rho}\left[\bigwedge^s (R^n)^* \otimes \bigwedge^{\rho+s} R^m\right] \longrightarrow \bigwedge^\rho R^m \longrightarrow \bigwedge^\rho R^n$$

We get a complex $K = K(\rho, b)$ of length $m - n + 1$ (reducing to the Koszul complex for $n = 1$). This may be generalized to a linear map $f\colon P \longrightarrow Q$ where P and Q are projective modules of constant ranks m, n $(m \geq n)$.

Let E be an A-module. Let $I(f) = \mathrm{Ann}\,(\mathrm{coker} \bigwedge^n f)$. Then:

Th.1
1) The I(f)- depth d of E is the smallest q such that $H^q(K,E) \neq 0$
2) $H^d(K,E) = \mathrm{Ext}^d\,(\mathrm{coker} \bigwedge^n f,\ E)$

Corollary - K is acyclic iff either the I(f) - depth of R is $m - n + 1$, or f is onto.

This gives informations about the projective varieties defined by the vanishing of the $(n \times n)$ minors of an $(m \times n)$ - matrix $(m \geq n)$

Th. 2 - If $H_i(K,E) = 0$, then $H_j(K,E) = 0$ for every $j \geq i$.

This affords evidence toward M. Auslander's conjecture quoted in § 4.

Th. 3 - If R is a Macaulay ring and if the I(f) - depth of R is $m - n + 1$, then $\mathrm{coker} \bigwedge^\rho f$ is unmixed.

This generalizes a well known theorem of Macaulay.

Finally let E be an R-module such that $(\operatorname{coker} f) \otimes E$ has finite length. Let $S_j(f)$ be the extension of f to the j-th symmetric powers. Then the length $\ell(\operatorname{coker} S_j(f) \otimes E)$ is finite, and is a polynomial $P_f(j, E)$ for j large. Its degree is $n - 1 + \dim E$ and is $\leq m$. Its leading coefficient depends only on coker f and E.

Th. 4 - The integer $\binom{n-1}{n-p} \frac{d^m}{dt^m} (P_f(t,E))$ is the Euler-Poincaré characteristic $\chi(H_*(K, E))$

Thus, if $n - 1 + \dim E = m$, this Euler-Poincaré characteristic may be viewed as a multiplicity.

§ 8. A weak form of Artin's conjecture. (N. Greenleaf)

This is a report on an unpublished paper of Ax and Kochen. Artin conjectured that any p-adic field K is C_2, i.e. that every homogeneous polynomial over K, with degree d and $n > d^2$ variables, has a non-trivial zero in K. Lang proved that a power-series field in one variable over a finite field is C_2. The theorem proved by Ax and Kochen is weaker than Artin's conjecture:

Theorem - Let d and n be integers such that $n > d^2$. There exists a finite set of primes $P_0 = P_0(d, n)$ such that, for every prime $p \notin P_0$ and every homogeneous polynomial $F(x_1, \ldots, x_n)$ of degree d over $\mathbb{Q}_p$, $F(x_1, \ldots, x_n)$ has a non-trivial zero in $\mathbb{Q}_p$.

Remark - N. Greenleaf proved a result which is stronger in some respects: given a homogeneous polynomial F over $\mathbb{Q}$, with degree d and $n > d$ variables (not d^2), F has a non-trivial zero in $\mathbb{Q}_p$ for almost all primes p.

The proof of the theorem is highly transfinite. Let P be the set of all primes and A the ring $\prod_{p \in P} \mathbb{Q}_p$. For $x = (x_p) \in A$, we set $N(x) = \{ p \in P \mid x_p \neq 0 \}$. If $\mathfrak{a}$ is an ideal $\neq A$, the family $(N(x))_{x \in \mathfrak{a}}$ is a filter over P, which determines $\mathfrak{a}$ completely; this filter is an ultrafilter U iff $\mathfrak{a}$ is maximal. Now consider $A' = \prod_{p \in P} \mathbb{F}_p((X))$, a non-trivial ultrafilter U over P and the corresponding maximal ideals m in A and m' in A'. One proves that the residue fields A/m and A'/m' are isomorphic [both are fields with valuations; both residue fields are isomorphic to $(\prod_{p \in P} \mathbb{F}_p) / \bar{m}$, where $\bar{m}$ is the maximal ideal of $\prod_{p \in P} \mathbb{F}_p$ corresponding to the ultrafilter U; they have characteristic 0; the fields are maximally complete]. Hency, by Lang's theorem, every polynomial of degree d in n variables over A/m has a non-trivial zero.

Remark - The authors use here the continuum hypothesis, but logicians have proved that it is harmless.

Suppose the theorem is false. Then the set I of all $\mathfrak{p} \in P$, for which there exists a homogeneous polynomial $F_{\mathfrak{p}}(X)$ of degree d in n variables over $Q_{\mathfrak{p}}$ with only the trivial zero, is infinite. For $\mathfrak{p} \in I$ let $F_{\mathfrak{p}}(X)$ be such a polynomial; for $q \notin I$ set $F_q(X) = 0$. Then $(F_{\mathfrak{p}}(X))_{\mathfrak{p} \in P}$ may be viewed as a polynomial $F(X)$ over A (since the polynomials $F_{\mathfrak{p}}(X)$ have the same degree; bounded degrees would do). Let U be a non-trivial ultrafilter containing I, and m the corresponding maximal ideal. The reduced polynomial $\bar{F}(X)$ over A/m has a non-trivial zero $(\bar{x})$. We lift $(\bar{x})$ to an element $(x) = (x_1, \ldots, x_n)$ of A^n, say $(x) = ((x_{\mathfrak{p}}))_{\mathfrak{p} \in P}$ with $(x_{\mathfrak{p}})$ in $Q_{\mathfrak{p}}^n$. We have $F(x) = (F_{\mathfrak{p}}(x_{\mathfrak{p}}))_{\mathfrak{p} \in P} \in m$; thus the set j of all $\mathfrak{p} \in P$ such that $F_{\mathfrak{p}}(x_{\mathfrak{p}}) = 0$ belongs to U. One of the components, say $x_1 = (x_{1,\mathfrak{p}})_{\mathfrak{p} \in P}$ of x is not in m; thus $N(x_1) \notin U$, whence $P - N(x_1) \in U$. Since U is a filter, $I \cap j \cap (P - N(x_1))$ is non-empty; let $\mathfrak{p}$ be one of its elements. We have $(x_{\mathfrak{p}}) \neq 0$ (since $x_{1,\mathfrak{p}} \neq 0$), $F_{\mathfrak{p}}(x_{\mathfrak{p}}) = 0$ (since $\mathfrak{p} \in j$), and $F_{\mathfrak{p}}(x_{\mathfrak{p}}) \neq 0$ (since $\mathfrak{p} \in I$). Contradiction.

BABY SEMINAR ON ÉTALE COHOMOLOGY

by

R. Hartshorne

In the baby seminar on étale cohomology, Steve Kleiman gave three lectures on the first two chapters of Mike Artin's notes ["Grothendieck Topologies", Harvard 1962]. He defined a topology, discussed presheaves, and proved Kan's theorem on the existence of the adjoint f_p to the "direct image" functor f^p. He then defined sheaves and proved useful properties of the category of sheaves (e.g. the existence of enough injectives). He defined cohomology and discussed the Leray spectral sequence.

Dan Quillen gave two lectures on the étale cohomology of sheaves over Spec k, a field. He showed the connection with the cohomology of profinite groups, and proved the theorem that if K/k is a finitely generated field extension, then

$$cd_p(K) \leq cd_p(k) + \text{tr.d.}(K/k),$$

where p is prime to the characteristic of k, and cd_p denotes the cohomological dimension for p-torsion sheaves.

REPORT ON THE WOODS HOLE FIXED POINT THEOREM SEMINAR

by

M. Atiyah and R. Bott

1) Introduction

This seminar was devoted to the discussion of a beautiful extension of the Lefschetz fixed point theorem which was proposed to the conference by Shimura. Shimura also noted that for curves this extension was a consequence of a result of Eichler.

Through the considerable advertising abilities of the authors a large number of the participants of the conference were drawn into the consideration of this formula and as a consequence of this intervention, especially that of Verdier, Mumford and Hartshorne, it was found that in the algebraic case the Shimura formula was correct and followed along more or less classical lines from the Grothendieck version of Serre duality.

The formula in question is the following one. Suppose that X is a non-singular projective algebraic variety over an algebraically closed field k, and that $f: X \rightarrow X$ is a morphism of X into itself. Suppose further that E is a vector bundle over X, and that f admits a lifting ϕ to E - that is, a vector bundle map $\phi: f^{-1}(E) \longrightarrow E$. Such a lifting then defines in a natural way an endomorphism $(f, \phi)^*$ of the cohomology vector-spaces $H^*(X;\underline{E})$, of X with coefficients in the locally free sheaf $\underline{E}$ of germs of sections of E, and we may therefore form the "Lefschetz number" of this endomorphism:

$$(1.1) \qquad \chi(f, \phi, E) = \sum_q (-)^q \text{ trace } \left\{ (f, \phi)^* \mid H^q(X ; \underline{E}) \right\} .$$

Suppose next that f is nondegenerate in the sense that the graph of f intersects the diagonal transversally in $X \times X$. This implies that at each fixed point p, of f, the differential $df_p : X_p \longrightarrow X_p$ has no eigenvalue equal to 1, so that $\det(1 - df_p) \neq 0$.

Finally note that at a fixed point p, the lifting ϕ determines an endomorphism ϕ_p of $E_p = E_{f(p)}$ and so has a well determined trace.

With this understood the Shimura conjecture which we now propose to call the Woods Hole Fixed Point Theorem, is given by the relation:

$$(1.2) \qquad \chi(f, \phi, E) = \sum_p \text{ trace } \phi_p / \det (1 - df_p)$$

where p runs over the fixed points of f.

2) Some examples

(2.1) As a first application of (1.2) we derive the usual Lefschetz formula for f when X is defined over the complex number field $\mathbb{C}$. For this purpose let T^* be the cotangent bundle of X, and let $\lambda^q T^*$ be its qth exterior power. The qth exterior power of the differential of f then defines a natural lifting, $\lambda^q df : f^{-1}(\lambda^q T^*) \longrightarrow \lambda^q T^*$ of f so that (1.2) is applicable and yields the identity:

$$\chi(f, \lambda^q df, \lambda^q T^*) = \sum_p \text{trace } (\lambda^q df_p) / \det(1 - df_p). \tag{2.2}$$

One now takes the alternating sum with respect to q. By virtue of the identity

$$\sum (-1)^q \text{ trace } \lambda^q df = \det(1 - df). \tag{2.3}$$

The right-hand side then counts the number of fixed points of f, each with multiplicity + 1, as indeed they should be counted in this nondegenerate and orientation preserving situation. The left hand side becomes $\sum (-1)^q$ trace $\{ f^* \mid H^q(X ; C) \}$ by virtue of the Dolboux isomorphisms. In short (2.2) implies the usual Lefschetz formula.

(2.4) Let P be projective n-space over K, with homogeneous coordinates $(x_0, \ldots\ldots, x_n)$. Let $f : P \longrightarrow P$ be the linear map, which sends x_i into $\lambda_i x_i$; $\lambda_i \neq 0$, $\lambda_i \neq \lambda_j$ if $i \neq j$.

The fixed points of f then correspond to the coordinate axes and are represented by $p_k = (0, \ldots, 1, \ldots, 0)$; $1 = 0, \ldots, n$; where the 1 occurs at the k^{th} place. Now $\det(1 - df_p)$ is easily computed to be

$$\prod_{j \neq k} (1 - \lambda_j / \lambda_k) .$$

Thus for instance, if we take the trivial bundle for E, and lift f to E by means of the constant section, then (1.2) takes the form:

$$1 = \sum_{k=0}^{n} \frac{\lambda_k^n}{\prod_{i \neq k} (\lambda_k - \lambda_i)}$$

which is a well-known interpolation formula.

If one takes for E the k power of the Hyperplane bundle, then may be lifted to E, in such a manner that the action of (f , ϕ) on $\Gamma(P; E) = H^*(P; \underline{E})$

is precisely the action induced on the polynomials of degree K in $K[x_0, \ldots\ldots, x_n]$ by the substitution $x_i \longrightarrow \lambda_i x_i$.

The formula (1.2) applied to this situation simultaneously for all k then yields the identity of formal power series in t:

$$\prod \frac{1}{(1 - t\lambda_j)} = \sum \frac{\lambda_k^n}{\prod_{i \neq k} (\lambda_i - \lambda_k)} \cdot \frac{1}{1 - t\lambda_k} . \tag{2.5}$$

This partial fraction expansion of the left-hand side is useful in the discussion of the characters of the irreducible representations of the full linear group, and indeed if one follows this lead, then (1.2) is seen to imply the formula of Herman Weyl for the character of an irreducible representation of a semi-simple Lie group in a most natural manner.

Our last example deals with the case when X is defined over a finite field of characteristic p. One may then use the Frobenius endomorphism for f (which is always nondegenerate!), and using the constant lifting of f to the structure sheaf, $0_X = \underline{1}$, one concludes directly from (1.2) that if X is "regular" in the sense that $H^i(X, O_X) = 0$; for $i > 0$, then X must have at least one rational point.

3) Remarks

It is not difficult to propose generalizations of (1.2). One may drop the non-degeneracy assumption on f, or remove the nonsingularity hypothesis on X; the vector bundle E may by replaced by a coherent sheaf, and finally—alas—with all this generality one may seek a statement relative to any proper morphism, rather then the projection onto a point.

The first step already leads to an interesting framework of ideas, and should shed new light on the problem of Riemann-Roch which corresponds to a highly degenerate f—namely the identity.

For a possible singular X one would at least hope to find a weak version of (1.2), i.e., that $\chi(f, \phi, E) = 0$ if f has no fixed points. A straightforward proof of this fact, that is, one not involving duality, would be highly desirable.

The authors' main personal concern was an extension of (1.2) along different lines. We consider an elliptic complex

$$\mathcal{E} : \; 0 \longrightarrow \underline{E}_0 \xrightarrow{d} \underline{E}_1 \xrightarrow{d} \cdots \underline{E}_m \longrightarrow 0$$

of C^∞ vector bundles E_i over a compact C^∞ manifold X, with differential operators

$d : \underline{E}_i \longrightarrow \underline{E}_{i+i}$ subject to $d^2 = 0$, and the ellipticity condition that the associated symbol sequence :

$$0 \longrightarrow E_0 \xrightarrow{\sigma(d,\xi)} E_1 \xrightarrow{\sigma(d,\xi)} \cdots E_m \longrightarrow 0$$

should be exact for every nonzero cotangent vector.

Under this hypothesis the complex $\Gamma(\mathcal{E})$ formed by the C^∞ -sections, $\Gamma(E_i)$ of E_i with differential operator $\Gamma(d)$, has finite-dimensional homology and a formula which specialized to (1.2) when $\mathcal{E}$ is the $\bar{\partial}$ resolution of $\underline{E}$ can be found. Details of this, and other developments will appear elsewhere.