III

AMERICAN MATHEMATICAL SOCIETY

Lecture Notes Prepared in Connection with the

Seminars held at the

Summer Institute on

Algebraic Geometry

Whitney Estate, Woods Hole, Massachusetts

July 6 - July 31, 1964

The 1964 Summer Institute in Algebraic Geometry was sponsored by the following agencies:

Air Force Office of Scientific Research
National Science Foundation
Office of Naval Research
United States Steel Foundation

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 $u \cdot v = \sum_{i=1}^{N} u_i \cdot \bar{v}_i$ 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, $\pi : \pi^{-1}(V_0) \xrightarrow{\simeq} V_0$, and $V_0 \dashrightarrow G_{N,n}$ 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

$x \in V - \left\{0\right\}$, where $f : V \dashrightarrow \mathbb{C}^N$, 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 $\pi \cdot \widetilde{V}_0 \dashrightarrow V$ 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 $T^0_x(S_\varepsilon)$. Then one can see that $T^0_x(S_\varepsilon)$ is orthogonal to the vector $\overrightarrow{Ox}$, and $S_\varepsilon \cap V$ is transversal at x if and only if $T^0_x(S_\varepsilon)$ does not contain $T_x(V)$ $(= T^0_x(V))$. Thus we get $S_\varepsilon \cap V$ is transversal at $x \Leftrightarrow \tau(f\,;x) > 0 \Leftrightarrow \rho(f\,;x) < 1$. 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 $f \cdot X \hookrightarrow Y \times \mathbb{C}$ 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 $\widetilde{X}$ generated by $\mathcal{J}$, and $\widetilde{Y}$ the complex subspace of $\widetilde{X}$ defined by $\mathcal{J}$. The flatness of $\widetilde{Y} \longrightarrow Y$ (which is the condition (ES)) implies that every irreducible component of $\widetilde{Y}$ is mapped onto Y. This implies that for every point y of Y, $\widetilde{h}^{-1}(X_y)$ is equal to the closure of $\widetilde{h}^{-1}(X_y - \xi(y))$ in $\widetilde{X}$. Now I claim: $\tau(1 ; x)$ on $X - \xi(Y) \cong \widetilde{h}^{-1}(X - \xi(Y))$ extends continuously through $\widetilde{X}$, and the extension is zero at every point of $\widetilde{X} - \widetilde{h}^{-1}(X - \xi(Y)) = \widetilde{h}^{-1}(\xi(Y))$. 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) $\mathcal{J}\underline{\mathcal{O}}_{\widetilde{X}}$ is invertible as $\underline{\mathcal{O}}_{\widetilde{X}}$- modules; and (ii) $\mathcal{J}_0\underline{\mathcal{O}}_{\widetilde{X}}$ is invertible, so that the natural map $X - \xi(Y) \longrightarrow Y \times G_{N,n}$ (cf. Remark (1, 2)) is holomorphically extended to $\widetilde{X} \longrightarrow Y \times G_{N,n}$, where $X - \xi(Y)$ is identified with $\widetilde{X} - \widetilde{h}^{-1}(\xi(Y))$. 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 $\varepsilon(x, t)\, x^q$, $q \geq 0$, $\varepsilon(0, 0) \neq 0$ (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 $\varepsilon(x, t) \neq 0$ for all (x, t) such that $|x| < \delta$, $|t| < \delta$.

Notations:

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:

Theorem. There exists a homeomorphism Ψ of $E_0 \times T$ into A such that:

1) $\Psi(V_0 \times T) = V$.

2) For any $(x, y) \in E_0$ and $t \in T$, we have $\Psi((x, y) \times t) = (x, \phi(x, y, t), t)$, where ϕ is some continuous function on $E_0 \times T$.

3) The function ϕ has the following properties.

3a) $\phi(x, y, 0) = y$.

3b) ϕ is analytic in t.

3c) ϕ is real analytic in x, y, t, except perhaps 1) at the points where $x = 0$ and 2) at the points of $V_0 \times 0$.

The construction of the function $\phi(x, y, t)$.

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

$$(2) \qquad \begin{aligned} \phi_1(x, \eta, t) &= y_i(x,t) \qquad \text{if } x \neq 0 \\ \phi_1(0,0,t) &= 0 . \end{aligned}$$

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_j 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:

$$(3) \quad \begin{cases} \phi(x, y, t) = y + \sum_{i=1}^{n} \sigma_i(x, y) \left[y_i(x,t) - \eta_i(x) \right] , \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } (x, y) \neq (0, 0) , \\ \phi(0, 0, t) = 0 . \end{cases}$$

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 $\mathcal{A}$ 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

$$(4) \quad \phi(x, y', t) \neq \phi(x, y, t) \text{ for all } x, y, y', t \text{ such that } |x| < \delta, \\ |t| < \delta \text{ and } y \neq y' .$$

The proof of (4) is based on two facts.

B1) By elementary calculus one shows that if $b_1, b_2, \dots, b_n$ are complex numbers and if

$$\gamma = \max\left\{\frac{|b_i - b_j|}{|y_i - y_j|}\right\} \qquad (y_i \neq y_j \text{ if } i \neq j)$$

then

$$(5)\ \left|\sum_i \left(\nu_i(y_1, y_2, \dots, y_n, y') - \nu_i(y_1, y_2, \dots, y_n, y)\right) b_i\right| \leq 4\gamma(n-1)\,|y'-y|.$$

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

$$(7)\qquad \frac{|\Delta_i(x,t) - \Delta_j(x,t)|}{|\eta_i(x) - \eta_j(x)|} \leq \gamma \qquad (\text{all } i, j,\ i \neq j),$$

then

$$(8)\qquad \left|\frac{\phi(x,y',t) - \phi(x,y,t)}{y' - y} - 1\right| \leq 4\gamma(n-1),$$

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:

Notations:

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 "direct product" assumption.

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 $\bar{P}$. From the "direct product" assumption follows that locally at $\bar{P}$, the fundamental group of $A' - \Delta$ is the same as the fundamental group of $A'' - \Delta_{\bar{t}}$, where A'' is the hyperplane $t = \bar{t}$ and $\Delta_{\bar{t}}$ is the section of Δ 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 A (where $E_0 = \{(x_1, x_2, \ldots, x_s, y)\} \,\big|\, |x_i| < \delta$, $i = 1, 2, \ldots, s$, δ sufficiently small), then it is necessary to assume that all the quotients

$$\frac{y_i(x,t) - y_j(x,t)}{y_i(x,0) - y_j(x,0)}, \qquad i \neq j,$$

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 $\epsilon(x_1, x_2, \ldots, x_s, t) D_0(x_1, x_2, \ldots, x_s)$ with $\epsilon(0, 0, \ldots, 0) \neq 0$.

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

Definition 1. 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

Notation. 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.

THEOREM. *Let* L *be a Galois extension of* K *of degree* p *and let* v *be a real nondiscrete valuation of* K *dominating* R *such that* v *has only one extension to* L. *Let* R_n *be the* n^{th} *quadratic transform of* R *along* v. *Then there exists a positive integer* m *such that for all* $n \geq m$ *we have that* ord_{R_n} *has only one extension to* L.

In turn, the proof of the above theorem follows from the following three lemmas.

Definition 2. 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)-*type* (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 $h: R \dashrightarrow R/xR$ is the natural epimorphism; $u > 0$, $a < p$, $b < p$, $c \leq 1$; if $a = 0$ then $b - c \not\equiv 0(p)$. if $c = 1$ then $b = 0$; if $b \neq 0$ then $v \neq 0$.

Definition 3. Given a monic polynomial $f(Z)$ in Z with coefficients in K we shall say that $f(Z)$ is R-*typical* 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).

Definition 4. Given a Galois extension L of K we shall say that L is *nice* 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.

Definition 5. 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-*translate* 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. *Let L be a Galois extension of K of degree p and let v be a real nondiscrete valuation of K dominating R such that v has only one extension to L. Let R_n be the n^{th} quadratic transform of R along v. Then there exists a positive integer m such that L is nice relative to R_m.*

LEMMA 2. *Let L be a Galois extension of K such that L is nice relative to R. Then ord_R has only one extension to L.*

LEMMA 3. (Stability). *Let $f(Z)$ be a monic polynomial of degree p in Z with coefficients in R such that $f(Z)$ is R-typical. Then given any quadratic transform S of R there exists an S-translate $g(Z)$ of $f(Z)$ such that $g(Z)$ is S-typical.*

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 $\mathbf{E}$ be a vector bundle of rank r over a curve C.

Definitions:

i) $\mathbf{E}$ is regular if the only endomorphisms of $\mathbf{E}$ are multiples of the identity.

ii) $\mathbf{E}$ is stable if, for all sub-bundles $\mathbb{F} \subset \mathbf{E}$, $\deg\left[c_1(\mathbb{F})\right] < \frac{\text{rank }(\mathbb{F})}{\text{rank }(\mathbf{E})} \cdot \deg\left[c_1(\mathbf{E})\right]$.

iii) $\mathbf{E}$ is semi-stable if, for all sub-bundles $\mathbb{F} \subset \mathbf{E}$, $\deg\left[c_1(\mathbf{F})\right] \leq \frac{\text{rank }(\mathbb{F})}{\text{rank }(\mathbf{E})} \cdot \deg\left[c_1(\mathbf{E})\right]$.

iv) $\mathbf{E}$ is retractable if it is a direct sum of stable bundles.

If $\deg\left[c_1(\mathbf{E})\right] = 0$, $\mathbf{E}$ is retractable if and only if $\mathbf{E}$ 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 $\deg\left[c_1(\mathbf{E})\right] = 0$; 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 compact 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. Compact moduli spaces for abelian varieties: Satake

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 ½-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:

$$V_n^{-*} = V_n^- \cup V_{n-1}^- \cup \cdots\cdots \cup V_1^- \cup V_0^-$$

(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:

$$\begin{tikzcd}
\left\{\begin{array}{c}\text{Stable } X \text{ with}\\ \text{polarization}\end{array}\right\} \arrow[r, phantom, "\cong"] \arrow[d, phantom, "\cap" rotate=180] & \left\{\begin{array}{c}\text{points of}\\ V_n^-\end{array}\right\} \arrow[d, phantom, "\cap" rotate=180] \\
\left\{\begin{array}{c}\text{retractable } X\\ \text{with polarization}\end{array}\right\} \arrow[r, phantom, "\cong"] \arrow[d, phantom, "\cap" rotate=180] & \left\{\begin{array}{c}\text{points of}\\ V_n^{-*}\end{array}\right\} \\
\left\{\begin{array}{c}\text{semi-stable } X\\ \text{with polarization}\end{array}\right\} \arrow[ur] &
\end{tikzcd}$$

<u>Explanations</u>

1° 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° A family of these objects is a morphism

$$f : \mathbf{X} \longrightarrow S$$

with the structure of group scheme (i.e., a "multiplication" $\mu : \mathbf{X} \underset{S}{\times} \mathbf{X} \longrightarrow \mathbf{X}$, etc.) and a family of Cartier divisors $\mathfrak{D}$ on $\mathbf{X}$ determined up to algebraic equivalence, and replacements

$$\mathfrak{D}' = \mathfrak{D} + f^*(\xi)$$

for any Cartier divisors ξ on S, and inducing a polarization of each fibre $f^{-1}(s)$. With this definition, stable and semi-stable $\mathbf{X}$'s form open sets, but retractable $\mathbf{X}$'s do not.

3° The meaning of the arrows in the diagram is this: let $f : \mathbf{X} \longrightarrow S$ 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 $\left\{ z \;\middle|\; |z| < 1 \right\}$ 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):

$$\Omega_{ij}(z) = \frac{1}{2\pi i} \log z \left(\begin{array}{c|c} S & 0 \\ \hline 0 & 0 \end{array}\right) + \left(\begin{array}{c|c} A(z) & B(z) \\ \hline {}^{t}B(z) & C(z) \end{array}\right)$$

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 $z \rightarrow 0$.

§ 3. Compact moduli spaces for curves

Let M_g denote the moduli scheme for curves of genus g. Let

$$\Theta : M_g \longrightarrow \overline{V}_g$$

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 $\overline{V}_g$, which we also denote M_g'. The simplest approach to compactifying M_g' is to use its closure M_g^* in $\overline{V}_g^*$. 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

$$M_g^* = M_g \cup M_g' \cup M_{g-1} \cup M_{g-1}' \cup \text{-------} \cup M_0$$

($M_0 = \overline{V}_0$ 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 $f : \mathcal{X} \longrightarrow C$ be a family of curves of arithmetic genus g $\Big[$i.e., f is proper and flat and its fibres $f^{-1}(P)$ are connected curves of arithmetic genus $g\Big]$. Let $P_0 \in C$ and assume that $f^{-1}(P)$ is non-singular if $P \neq P_0$. Then there exists a diagram:

$$\begin{tikzcd}
\mathcal{X}' \arrow[r, "\pi'"] \arrow[d, "f'"'] & \mathcal{X} \arrow[d, "f"] \\
C' \arrow[r, "\pi"'] & C
\end{tikzcd}$$

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) $\mathfrak{X}' - f'^{-1}(P_0')$ is just the induced family of curves over $C' - P_0'$, i.e.

$$(C' - P_0') \times_C \mathfrak{X} = \mathfrak{X}' - f'^{-1}(P_0'),$$

4) $f'^{-1}(P_0')$ is reduced and has only ordinary double points.

Lemma B: Let C be a curve and let

$$f : \mathfrak{X} \longrightarrow C$$

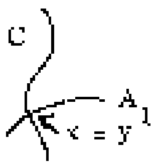
be a family of curves of arithmetic genus g such that each curve $f^{-1}(P)$ is reduced and has only ordinary double points. Then the set of generalized jacobian varieties of the curves $f^{-1}(P)$ forms a family of polarized semi-stable group varieties over C.

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: $\tilde{M}_g^*$. It is still unknown whether $\tilde{M}_g^*$ is a projective algebraic variety, although it is a Q-variety. There is a proper holomorphic map

$$\tilde{M}_g^* \longrightarrow M_g^*$$

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 V_n^* so as to obtain a $\tilde{V}_n^*$ which corresponds to a moduli problem with a larger set of stable objects. We would like the stable points of $\tilde{V}_n^*$ 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,

$$\left\{\begin{matrix}\text{points of}\\ J\end{matrix}\right\} = \left\{\begin{matrix}\text{invertible sheaves } L \text{ on } C\\ \text{such that } \chi(L) = \chi(\mathcal{O}_C)\end{matrix}\right\} .$$

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

$$\begin{array}{ccc}\left\{\begin{matrix}\text{points of}\\ J\end{matrix}\right\} & \cong & \left\{\begin{matrix}\text{invertible sheaves } L \text{ on } C\\ \text{such that } \chi(L) = \chi(\mathcal{O}_C)\end{matrix}\right\} \\ \cap & & \cap \\ \left\{\begin{matrix}\text{points of}\\ J^*\end{matrix}\right\} & \cong & \left\{\begin{matrix}\text{rank 1, torsion-free sheaves } \mathcal{F} \text{ on } C\\ \text{such that } \chi(\mathcal{F}) = \chi(\mathcal{O}_C)\end{matrix}\right\}\end{array} .$$

Using this, we find an interesting $\tilde{V}_2^*$, 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 G_m can be described by class field theory as follows:

Denote by

$$i: \text{Spec } k \longrightarrow U$$

the map. One has the usual exact sequence

$$0 \longrightarrow (G_m)_U \longrightarrow i_*(G_m)_k \longrightarrow D \longrightarrow 0 \tag{1.2}$$

where

$$D \quad \bigoplus_{\substack{x \text{ closed} \\ \text{in } U}} \quad (\mathbb{Z})_x$$

is the sheaf of Cartier divisors on U . Now by local class field theory.

$$R^q i_* \mathbb{G}_m = 0, \quad q > 0, \qquad \text{i.e.,} \tag{1.3}$$

$$H^q(U, i_* \mathbb{G}_m) \simeq H^q(\text{Spec } k, \mathbb{G}_m) \; ; \; \text{all } q \; .$$

Taking into account the vanishing of certain groups, the exact cohomology sequence of (1.2) yields the exact sequences

$$0 \longrightarrow \mathbb{G}_m(U) \longrightarrow k^* \longrightarrow \bigoplus_x (\mathbb{Z}) \longrightarrow \text{Pic } U \longrightarrow 0 \, , \tag{1.4}$$

$$0 \longrightarrow H^2(U, \mathbb{G}_m) \longrightarrow \text{Br } k \xrightarrow{\phi} \bigoplus_x (\mathbb{Q}/\mathbb{Z}) \longrightarrow H^3(U, \mathbb{G}_m) \longrightarrow 0$$

where $\mathrm{Br}\ k = \mathbf{H}^2(\mathrm{Spec}\ k, \mathbb{G}_m)$ 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) $$\mathrm{cd}_p Y \leq \mathrm{cdqc}\ Y + 1 \qquad (p = \mathrm{char}\ Y)$$

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): $$\mathrm{cd}_p X \leq 2\ \dim\ X + 1 \text{ if } p \neq 2 .$$

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 $X \sqcup X_\infty$ 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.

<u>Theorem (2.5)</u>: 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 $q > 2\dim X + 1$.

<u>Corollary (2.6)</u>: (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 $\underline{H}^q(X, F^\cdot)$ the hypercohomology of X into $F^\cdot$ and by $\underline{\underline{\mathrm{Ext}}}^q(X; F^\cdot, \mathbb{G}_m)$ 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.

<u>**Theorem (3.1)**</u>. The Yoneda product

$$(*)_p \quad \underline{\underline{H}}^q(X, F^\cdot)_p \times \underline{\underline{\mathrm{Ext}}}^{3-q}(X; F^\cdot, \mathbb{G}_m)_p \longrightarrow H^3(X, \mathbb{G}_m)_p \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p$$

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 $\underline{\underline{H}}^q_c(U, F^\cdot)$ (hypercohomology with compact support on U) by the equality:

$$\underline{\underline{H}}^q_c(U, F^\cdot) = \underline{H}^q(X, F^\cdot_U).$$

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 $\underline{\text{Rhom}}(F^{\cdot}, I(G^{\cdot}))$ to be the single complex of sheaves on U of sheaf homomorphism of $F^{\cdot}$ into $I(G^{\cdot})$. Then we define $\underline{\underline{\text{Ext}}}_c^q(U;F^{\cdot},G^{\cdot})$ by the equality:

$$\underline{\underline{\text{Ext}}}_c^q(U;F^{\cdot},G^{\cdot}) = \underline{\underline{H}}^q(X, \underline{\text{Rhom}}(F^{\cdot}, I(G^{\cdot}))_U).$$

When the complex $G^{\cdot}$ is the single sheaf $\mathbb{G}_m$, the complex $\underline{\text{Rhom}}(F^{\cdot}, I(\mathbb{G}_m))$ will be denoted by $D(F^{\cdot})$.

As an immediate corollary of the theorem 3.1 we obtain:

<u>Corollary 3.2</u>: The Yoneda product

$$\underline{\underline{H}}_c^q(U,F^{\cdot})_p \times \underline{\underline{\text{Ext}}}^{3-q}(U;F^{\cdot},\mathbb{G}_m)_p \longrightarrow \underline{\underline{H}}_c^3(U,\mathbb{G}_m)_p \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p$$

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

$$\triangle \quad F^{\cdot} \longrightarrow D(D(F^{\cdot})).$$

<u>Theorem 3.3</u>: 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.

<u>Corollary 3.4</u>: The Yoneda product

$$\underline{\underline{H}}^q(U,F^{\cdot})_p \times \underline{\underline{\text{Ext}}}_c^{3-q}(U;F^{\cdot},\mathbb{G}_m)_p \longrightarrow \underline{\underline{H}}_c^3(U,\mathbb{G}_m)_p \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p$$

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, *a one-parameter formal Lie group over A* 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 *A-homomorphism of F into G* 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.

Proposition. If A is an integral domain of characteristic zero, and F a formal group over A, the map

$$c : \mathrm{End}_A(F) \to A$$

is an injective ring-homomorphism.

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 $\mathbf{Z}_p$, the p-adic integers.

Proposition. If F is a formal Lie group defined over the $\mathfrak{p}$-adic integer ring $\mathfrak{o}$, and F^*, the formal group defined over $k = \mathfrak{o}/\mathfrak{p}$ by reducing all the coefficients of F modulo $\mathfrak{p}$, is such that F^* is not k-isomorphic to the additive formal group $x + y$, then $\mathrm{End}_{\mathfrak{o}}(F)$ is injected into $\mathrm{End}_k(F^*)$ by the reduction map $f \mapsto f^*$.

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 $\mathbf{Q}_p$. 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 $\mathscr{O}$ 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 $\mathscr{O}$, 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 $\mathscr{O}$, 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 $\mathrm{End}(F) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = K$-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 $\mathcal{A}$, there is a full formal group F defined over $\mathcal{A}$ whose absolute endomorphism ring is isomorphic to $\mathcal{A}$. Then $T(F)$ is a free $\mathcal{A}$-module of rank 1 and so $G = \mathcal{G}(\mathcal{L}/K) \hookrightarrow GL(1, \mathcal{A}) = \mathcal{A}^*$. 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 $\mathcal{A}^*$ 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 $u \in \mathcal{A}^*$,

$$(u, \mathcal{L}/K)(\alpha) = [u^{-1}]_F(\alpha).$$

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 $k = \mathcal{A}/\mathcal{P}$. 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 $\mathcal{A}[t_1, \ldots, t_{h-1}]$ 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 $\mathcal{A}$-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 $k = \mathcal{A}/\mathcal{P}$, 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* $\phi: F \cong \Gamma(\alpha)$ *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 $\mathcal{O}$-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 $\mathcal{O}[[t_1, \ldots, t_{h-1}]]$. As usual there results an operation of Aut Φ on $\mathcal{O}[[t]]$, whose study should be interesting. In case $h = 2$ we have used it to construct an elliptic curve E over $\mathcal{O}$ 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 $\mathcal{U}$ be an open covering of X. With the aid of the group law $X \times X \to X$ one can associate with $\mathcal{U}$ a certain open cover $\mathcal{U}^{(p)}$ of $X^p = X \times X \times \ldots \times X$ (p times), for each p. One can then define a double complex $C^{\cdot\cdot}(\mathcal{U}, X, B)$ in which an element of $C^{p,q}$ is a family of morphisms from the intersections of $(q+1)$ open sets in the covering $\mathcal{U}^{(p)}$ 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 $H^n(\mathcal{U}, X, B)$. For example, $H^2(\mathcal{U}, X, B)$ describes the group-scheme extensions of X by B which, as fiber spaces, are trivial on the covering $\mathcal{U}$. Passing to the limit over $\mathcal{U}$, 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 $\operatorname{Ker}(A \xrightarrow{p^n} A)$ 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

$$B' = B \otimes_R R', \quad X' = X \otimes_R R', \quad \tilde{B} = B \otimes_R k, \text{ etc.}$$

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 $\mathbf{G}_a$.

<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

$$0 \to C^{\cdot\cdot}(\mathfrak{U}, \widetilde{X}, W) \to C^{\cdot\cdot}(\mathfrak{U}, X, B) \to C^{\cdot\cdot}(\mathfrak{U}, X', B') \to 0 ,$$

where $\mathfrak{U}$ 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):

$$A^* = \lim_{n \to \infty} A_{p^n} \quad \text{where } A_{p^n} = \mathrm{Ker}\,(p^n : A \to A) .$$

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 $(\widetilde{A}, A^*)$ where $\widetilde{A}$ is the reduction of $A \pmod{m}$ which is an abelian variety over k. Clearly, A^* is a raising of $(\widetilde{A})^*$. The marvellous thing is that it is an equivalence of categories. In other words, if one knows the reduction $\widetilde{A}$ of an abelian scheme A all that is lacking to determine A is a raising of the ind-group scheme $\widetilde{A}^*$ which is quite an innocent thing (see below).

The proof of the theorem which was sketched in the seminar used the exact sequence of (1) 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,

$$0 \to A^*_{m} \to A^* \to A^*_{\text{ét}} \to 0$$

where A^*_{m} and $A^*_{\text{ét}}$ are the canonical raisings of Φ^*_{m} and $\Phi^*_{\text{ét}}$. 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 finite order deserve the name quasi-canonical. 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 $T_p \otimes \mathbb{Q}_p$ splits 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

$$\theta : k - \operatorname{Ker}(\text{Hasse}) \to W(k)$$

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'.

Theorem (i) Let $\lambda \in k - \mathrm{Ker}\,(\mathrm{Hasse})$, and let $x = \theta(\lambda) \in W(k)$. One has

(*) $$T_p(x, s(x)) = 0, \text{ and } x \equiv \lambda \pmod{p}$$

(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, Sur les groupes de Lie formels à un paramètre. Bull. Soc. Math. France 83 (1955), p. 251-274.

[2] J. Lubin, One-parameter formal Lie groups over $\mathfrak{p}$-adic integer rings. Annals of Math. to appear.

[3] J. Lubin and J. Tate, Formal complex multiplication in local fields. Annals of Math. to appear.

[4] J.P. Serre, Groupes de Lie ℓ-adiques attachés aux courbes elliptiques. 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 $p: G \to X$ 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:

$$\begin{tikzcd}
V \arrow[d, "\pi"] & & X \times F \arrow[ll, "\text{the natural map} = \tilde{p}"'] \arrow[d, "\tilde{\pi}"] \arrow[r, phantom, "\ni"] & (x, u) \arrow[d, maps to] \\
U & & X \arrow[ll, "\text{the natural map} = p"'] \arrow[r, phantom, "\ni"] & x
\end{tikzcd}$$

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 $T \in \mathfrak{p}$. (7) $d\rho(Z) S - S d\rho(Z) = 0$ for all $Z \in \mathfrak{k}$, 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 $\{ (F, J(x)) \ x \in X \}$. 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 $\mathfrak{k}$, 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 $\mathfrak{K}/\mathfrak{k}$ let $f_{\mathfrak{p}}$ denote the degree of $\mathfrak{p}$ over $\mathfrak{k}$. 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

$$L(\mathfrak{K}'/\mathfrak{K},\ R;\ u) = \prod_{\mathfrak{P}} \det(1 - R(\sigma_{\mathfrak{P}})u^{f_{\mathfrak{P}}})^{-1}.$$

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 $\widetilde{W}_N^{\mathfrak{p}(1)}$ of $W_N^{(1)}$ modulo $\mathfrak{p}$ has also a structure of fibre variety over $\widetilde{V}_N^{\mathfrak{p}}$, whose fibres are abelian varieties $\widetilde{A}_x$ of dimension 2. Take a generic point x of $\widetilde{V}_N^{\mathfrak{p}}$ over the prime field κ , and consider the fibre $\widetilde{A}_x$ of $\widetilde{W}_N^{\mathfrak{p}(1)}$ at x . For a prime number $\ell \nmid \mathfrak{p}$, 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,

$$(1)\qquad L(\mathfrak{K}'/\mathfrak{K}, \underbrace{\square\square\square\square\square}_{n} \circ \mu_\ell', u) = \begin{cases} H^N_{n+2}(p, u) & (n>0) \\ H^N_2(p, u)\,/\,(1-u)(1-pu) & (n=0)\ . \end{cases}$$

where $H^N_m(p, u) = \det(1 - T^N_m(p)u + pT^N_m(p.p)u^2)$ (cf. [ZF]).

From this equality (1) we can deduce the following results. The normal subgroup $\Gamma_{N\ell}(\mathfrak{O})$ of $\Gamma_K(\mathfrak{O})$ defines a covering Riemann surface $\Gamma_{N\ell}(\mathfrak{O})\backslash X$ of $\Gamma_K(\mathfrak{O})\backslash X$. 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 $p \equiv 1 \mod \ell$,

$$(2)\qquad f_p = \text{some power of } \ell\ (= 1 \text{ or } \ell, \text{ or } \ell^2 \ldots)$$

$$\Longleftrightarrow \begin{cases} H^N_{n+2}(p, u) \equiv (1-u)^{2d_{n+2}} \mod \ell, \\ \text{for } n = 0, 2, 4, \ldots\ldots, \ell-1, \quad \text{where} \end{cases}$$

d_m = the dimension of the space of holomorphic $\Gamma(\mathfrak{O}, N)$ - automorphic forms of weight m .

Our method cannot be applied for $\Gamma = SL(2, \mathbb{Z})$, because we assumed that $\Gamma \backslash X$ is compact. But we may conjecture that the same result (2) holds also for $SL(2, \mathbb{Z})$. If we assume this, we can deduce the following relations for the Ramanujan's function $\tau(p)$, where $x \prod_{n=1}^{\infty} (1 - x^n)^{24} = \sum_{n=1}^{\infty} \tau(n) x^n$.

(i) $p \equiv 1 \ (3)$ implies $\tau(p) \equiv 2 \ (3)$,

(ii) $p \equiv 1 \ (5)$ implies $\tau(p) \equiv 2 \ (5)$,

(iii) $p \equiv 1 \ (7)$ 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 $\left\{ p \text{ rational prime number} \ \middle| \ p \equiv 1 \ (\ell) ,\ \tau(p) \equiv a \ (\ell) \right\}$ 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) *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.*

Such a k_0 is uniquely determined by $\mathcal{Q}$ and is called *the field of moduli of* $\mathcal{Q}$.

§ 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 ρ 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, ρ) 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 $\theta(a) \longrightarrow \theta(a^\rho)$ on $\theta(S)$. Such a $\mathcal{P}$ does not exist unless the following condition is satisfied:

(2.1) *The direct sum of Φ and its complex conjugate $\overline{\Phi}$ is equivalent to a rational representation of S.*

Let $\mathcal{P} = (A, \mathcal{C}, \theta)$ be of type (S, Φ, ρ), 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 $(S, \Phi, \rho; T, L)$. If S is of (Type I, II, III), T can be arbitrary. Suppose that S belongs to (Type IV). Put $g = [F : Q]$. Let $\tau_1, \ldots, \tau_K$ 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) *For each ν, the complex hermitian matrix $\sqrt{-1}$ (T) has exactly r_ν negative characteristic roots.*

Let $u_1, \ldots, u_r \in W$. We say that $\mathfrak{Q} = \mathcal{P}(t_1, \ldots, t_r)$ is of type $(S, \Phi, \rho; T, L, \{u_i\})$ if $t_i = f(u_i) \bmod D$ for the above i.

Put $M = L + \sum_{i=1}^{r} Zu_i$, 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.

Theorem 1. If Φ satisfies (2.1) and T satisfies (2.2), then for a given $(S, \Phi, \rho; T, L; \{u_i\})$, there exists an analytic family $\Sigma = \{\mathfrak{Q}_z \mid z \in X\}$ with the following properties:

(1) Every member $\mathfrak{Q}_z$ is of type $(S, \Phi, \rho; T, L; \{u_i\})$.

(2) *Every* $\mathcal{Q}$ *of type* $(S, \Phi, u; T, L, U_i)$ *is isomorphic to a member of* $\sum$.

(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 $\sum$, 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 $S^* = Q(tr(\Phi(x)) \mid x \in S)$. 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 suitablely 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^*:

$$H = \left\{ \mathfrak{A} \;\middle|\; \prod_{\lambda=1}^{h} \left(\frac{\mathfrak{A}^{\sigma_\lambda}}{\mathfrak{A}^{\sigma_\lambda \rho}}\right)^{\nu_\lambda} = (y),\ y\bar{y} = 1,\ N(\mathfrak{A}) \equiv y \equiv 1 \mod^* \mathfrak{a} \text{ for an element } y \text{ of } S \right\} \quad \text{if } m \text{ is even;}$$

$$H = \left\{ \mathfrak{A} \;\middle|\; \prod_{\lambda=1}^{h} \mathfrak{A}^{\sigma_\lambda} \cdot \left(\frac{\mathfrak{A}^{\sigma_\lambda}}{\mathfrak{A}^{\sigma_\lambda \rho}}\right)^{\nu_\lambda} = (y),\ y\bar{y} = N(\mathfrak{A}),\ y \equiv 1 \mod^* \mathfrak{a} \text{ for an element } y \text{ of } S \right\}, \quad \text{if } m \text{ is odd.}$$

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

$$\Gamma(\mathfrak{O};\mathfrak{a}) = \left\{ x \in \mathfrak{O} \mid xx^{\iota} = 1,\ x \equiv 1 \mod \mathfrak{a}\mathfrak{O} \right\},$$

where ι is the canonical involution of D. Projecting $\Gamma(\mathfrak{O};\mathfrak{a})$ to the partial product $M_2(R)^t$, we may consicer it as a discontinuous group operating on $X^t = \left\{ (z_1, \ldots, z_t) \in C^t \mid \mathrm{Im}(z_1) > 0, \ldots, \mathrm{Im}(z_t) > 0 \right\}$.

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: (i) 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*

$$\left\{ \mathfrak{c} \mid \prod_{i=1}^{u} \mathfrak{c}^{\tau_i} \in I(D/F) \right\}$$

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 those 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' 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 $(P_\alpha, f_{\alpha\beta})$ of finitely presented modules: writing $0 \longrightarrow R \longrightarrow A^{(M \times \mathbf{Z})} \longrightarrow M \longrightarrow 0$, the indices α are pairs (I, S) where I is a finite subset of $M \times \mathbf{Z}$ 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 E_α of finite rank: $P_\alpha \longrightarrow E_\alpha \longrightarrow M$ (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 $P_\alpha \longrightarrow E_\alpha \longrightarrow M$. 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 $\Lambda(M)$ and the symmetric algebra $S(M)$ are flat A-modules. In particular, if A is an integral 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 rèflexifs 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, $d\beta(M)$ (or $d\beta_A(M)$) 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 $p \in \operatorname{Spec}(A)$, we have $d\beta_{A_p}(M_p) \geq \inf(q, d\beta_{A_p}(A_p)) = \inf(q, h(p))$

If M has finite homological dimension, these statements are equivalent to:

(P''_q) For every $P \in \operatorname{Spec}(A)$, 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 $0 \longrightarrow M \longrightarrow F_1 \longrightarrow F_2 \longrightarrow --- \longrightarrow F_q$ 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) $S(M)$ *is a domain iff* A *is a domain and each* $S^n(M)$ *is torsion free over* A (i.e., *has property* (P_1)).

2) $S(M)$ *is factorial iff* A *is factorial and each* $S^n(M)$ *is reflexive over* A (i.e., *has property* (P_2)).

3) $S(M)$ *is regular iff* A *is regular and each* $S^n(M)$ *is a projective* A-*module* (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 *homological dimension one*, i.e., defined by n generators x_i and $s \leq n$ linearly independent relations $\sum_{i=1}^{n} a_{ji}x_i = 0$. 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, $A\left[X_1 \ldots X_n\right] / (\sum_{i=1}^{n} a_i x_i)$ 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. *Power series over integrally closed domains.* (P. Samuel).

It is well known and easy to prove that, if A is *completely* 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 th

$$(Xu(X))^2 + a\,Xu(X) + X = 0$$

($au_0 - 1 = 0$, $u_0^2 + au_1 = 0$, $2u_0u_1 + au_2 = 0$, 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 $\sqrt{a^2+x} = a\sqrt{1+\frac{x}{a}} = a\left(1+\frac{x}{2a} - \frac{1}{8}\frac{x^2}{a^2} + \frac{1}{16}\frac{x^3}{a^3} \cdots\cdots\cdots\right)$

§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:

Theorem - If $\mathrm{Tor}_i(A,B) = 0$, then $\mathrm{Tor}_j(A,B) = 0$ for any $j \geq i$.

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 $\mathrm{hd}(A) + \mathrm{hd}(B) \leq \dim R$. Consequently, if the n-fold tensor product $A\otimes --- \otimes A$ ($n = \dim R$) 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 $\mathrm{hd}A = \mathrm{hd}A^*$, 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 $--- \longrightarrow X_i \longrightarrow X_{i+d} \longrightarrow X_{i+2d} \longrightarrow ---$, 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 $\mathrm{hd}_{R_p}(A_p) =$ (resp. $\leq$) $\mathrm{hd}_{R_p}(A^1_p)$ 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 $\mathrm{hd}_{R_p}(A_p) + \mathrm{hd}_{R_p}(B_p) \geq \dim(R_p) + i$. 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 $\mathrm{hd}(A) < q$, 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

$$(1) \qquad C \otimes_B \Omega_{B/A} \longrightarrow \Omega_{C/A} \longrightarrow \Omega_{C/B} \longrightarrow 0$$

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 <u>nine terms</u>. 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 <u>six-terms</u> exact sequence.

a) <u>Definition of the functors</u> (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 "<u>cotangent complex</u>" $L(B/A, P, F)$ 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 <u>define</u> $T_i(B/A, M) = H_i(L(B/A) \otimes M)$ 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) <u>Vanishing properties</u>

We have $T^1(B/A, M) = 0$ for every B-module M iff B is <u>formally smooth</u> 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 <u>locally a complete intersection</u> 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 <u>field extension</u>, 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 <u>separability</u> 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

$$0 \longrightarrow L(B/A, P, F) \otimes \hookrightarrow L(C/A, R, H) \longrightarrow L(C/B, Q, G) \longrightarrow 0$$

is "almost exact". As usual this gives an exact sequence:

$$T_2(B/A, M) \to T_2(C/A, M) \to T_2(C/B, M) \to T_1(B/A, M) \to T_1(C/A, M) \dashrightarrow T_0(C/B, M) \to 0$$

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 $T_i(\cdot, C)$: here the T_0-terms are 0, $T_2(C/B, C) = 0$ by the hypothesis on K, and the T_1-terms give:

$$0 \longrightarrow I/JI \longrightarrow J/J^2 \longrightarrow K/K^2 \dashrightarrow 0\ ;$$

by hypothesis J/J^2 and K/K^2 are free C-modules of ranks $\dim A - \dim C$ and $\dim B - \dim C$; whence, by Nakayama, I is generated by $\dim A - \dim B$ 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 isomorphism classes of such extensions correspond bijectively to the elements of $T^1(B/A, M)$

b) Deformations

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 infinitesimal deformation of B/A over A^1 is an A^1-flat algebra B^1 such that $B^1/jB^1 \simeq B$. 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:

$$0 \longrightarrow A = H^1(X, T^0) \longrightarrow B = F(k[\varepsilon]) \longrightarrow H^0(X, T^1) = b \longrightarrow H^2(X, T^0) \text{ - - }$$

(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 formal prescheme $\mathfrak{X}$ 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 non-canonical 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, basec 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 $T^1_P = \operatorname{Ext}^1(T^0_P, \mathcal{O}_P)$ 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

$$\ell_{X/Y} = \left[z^*\Omega_{P/Y} \right] - \left[I/I^2 \right]$$

This is the class of the Kähler-different of X/Y. With $X \xrightarrow{h} Y \longrightarrow Z$, we have the transitivity formula

$$\ell_{X/Y} = h^*(\ell_{Y/Z}) + \ell(X/Y)$$

The Chern-class $K_{X/Y} = c_1(\ell_{X/Y})$ in $\operatorname{Pic}(X)$ is interesting; it gives the good canonical class for a curve over a non-perfect field.

The Riemann-Roch formula

$$f_*(\mathrm{ch}\, x \cdot T(X)) = T(Y)\, \mathrm{ch}(f_* x)$$

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 $\mathbf{Z}\left[\,(X_{ij})\,\right] = S$, $(\rho - n)$. 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

$$0 \longrightarrow \overset{m}{\Lambda}\, S^m \longrightarrow \ \ldots\ldots \longrightarrow \overset{2}{\Lambda}\, S^m \longrightarrow S^m \longrightarrow S \longrightarrow S/(X_1,\ldots,X_m) \longrightarrow 0$$

More generally we have a commutative ring R and a linear map $f: R^m \longrightarrow R^n$ $(m \geq n)$, described by a matrix (x_{ij}). We consider $\overset{\rho}{\Lambda} f:\ \overset{\rho}{\Lambda} R^m \longrightarrow \overset{\rho}{\Lambda} R^n$ $(\rho \leq n)$ and have to extend it (on the left) to a free acyclic complex. This is an analogue of the bar-construction. First terms:

$$\ldots \longrightarrow \sum_{s > n-\rho} \left[\overset{s}{\Lambda}(R^n)^* \otimes \overset{\rho+s}{\Lambda} R^m\right] \longrightarrow \overset{\rho}{\Lambda} R^m \longrightarrow \overset{\rho}{\Lambda} R^n$$

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 $f: P \longrightarrow Q$ where P and Q are projective modules of constant ranks m, n $(m \geq n)$.

Let E be an A-module. Let $I(f) = \mathrm{Ann}\,(\mathrm{coker} \overset{n}{\Lambda} f)$. Then:

Th. 1 –
1) *The* $I(f)$– *depth* d *of* E *is the smallest* q *such that* $H^q(K, E) \neq 0$
2) $H^d(K, E) = \mathrm{Ext}^d\,(\mathrm{coker} \overset{n}{\Lambda} f,\ E)$

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* coker $\overset{\rho}{\Lambda} f$ *is unmixed*.

This generalizes a well known theorem of Macaulay.

Finally let E be an R-module such that (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 ℓ(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 Q_p, $F(x_1, \ldots, x_n)$ has a non-trivial zero in Q_p.

Remark - N. Greenleaf proved a result which is stronger in some respects: given a homogeneous polynomial F over Q, with degree d and $n > d$ variables (not d^2), F has a non-trivial zero in 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 $\prod_{p \in P} Q_p$. 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 $(\prod_{p \in P} \mathbb{F}_p) / \overline{m}$, where $\overline{m}$ 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 $\overline{F}(X)$ 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 $f : X \to X$ 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:

$$\chi(f, \phi, E) = \sum_q (-)^q \text{ trace } \left\{ (f, \phi)^* \mid H^q(X ; \underline{E}) \right\} . \tag{1.1}$$

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;

$$\chi(f, \phi, E) = \sum_p \text{ trace } \phi_p / \det(1 - df_p) \tag{1-2}$$

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:

$$(2.2) \qquad \chi(f, \lambda^q df, \lambda^q T^*) = \sum_p \ \text{trace} \ (\lambda^q \, df_p) \ / \ \det (1 - df_p).$$

One now takes the alternating sum with respect to q. By virtue of the identity

$$(2.3) \qquad \sum (-1)^q \ \text{trace} \, \lambda^q df = \det (1 - df).$$

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 $\left\{ f^* \mid H^q(X ; C) \right\}$ 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 $p_k = (0, \ldots\ldots, 1, \ldots\ldots, 0)$; $1 = 0, \ldots\ldots, n$; 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. $\phi_X = 1$. 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 nondegeneracy 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

$$\mathcal{E}: \; 0 \longrightarrow E_0 \xrightarrow{d} E_1 \xrightarrow{d} \cdots E_m \longrightarrow 0$$

of C^∞ vector bundles E_i over a compact C^∞ manifold X, with differential operators

$d : \underline{\mathbf{E}}_i \longrightarrow \underline{\mathbf{E}}_{i+1}$ subject to $d^2 = 0$, and the ellipticity condition that the associated symbol sequence :

$$0 \longrightarrow E_0 \xrightarrow{\sigma(c,\xi)} E_1 \xrightarrow{\sigma(d,\xi)} \cdots \quad E_m \longrightarrow 0$$

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 $\mathbf{E}_i$ with differential operator $\Gamma(d)$, has finite-dimensional homology and a formula which specialized to (I.2) when $\mathcal{E}$ is the $\bar{\partial}$ resolution of $\underline{\mathbf{E}}$ can be found. Details of this, and other developments will appear elsewhere.